University of Alberta

Jurisdictional Issues Raised by e-Commerce

by

Kathryn Louise Dykstra

A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfillment of the requirements for the degree of Master of Laws

Department of Law

Edmonton, Alberta

Spring, 2000

NEW.NEW;G:\dox\kld;877642.WPD;1

National Library of Canada
Acquisitions and Bibliographic Services
395 Wellington Street
Ottawa ON K1A 0N4
Canada

Bibliothèque nationale du Canada
Acquisitions et services bibliographiques
395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file Votre référence

Our file Notre référence

The author has granted a non-exclusive licence allowing the National Library of Canada to reproduce, loan, distribute or sell copies of this thesis in microform, paper or electronic formats.

L'auteur a accordé une licence non exclusive permettant à la Bibliothèque nationale du Canada de reproduire, prêter, distribuer ou vendre des copies de cette thèse sous la forme de microfiche/film, de reproduction sur papier ou sur format électronique.

The author retains ownership of the copyright in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

L'auteur conserve la propriété du droit d'auteur qui protège cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

0-612-60049-1

Canada

University of Alberta

Library Release Form

Name of Author: Kathryn Louise Dykstra

Title of Thesis: Jurisdictional Issues Raised by e-Commerce

Degree: Master of Laws

Year this Degree Granted: 2000

Permission is hereby granted to the University of Alberta Library to reproduce single copies of this thesis and to lend or sell such copies for private, scholarly, or scientific research purposes only.

The author reserves all other publication and other rights in association with the copyright in the thesis, and except as hereinbefore provided, neither the thesis nor any substantial portion thereof may be printed or otherwise reproduced in any material form whatever without the author's prior written permission.

14523 Summit Dr.
Edmonton, Alberta
T5N 3T3

Date submitted to the Faculty of Graduate Studies and Research

April 14, 2000

NEW.NEW;G:\dox\kld;877635.WPD;1

University of Alberta

Faculty of Graduate Studies and Research

The undersigned certify that they have read, and recommended to the Faculty of Graduate Studies and Research for acceptance, a thesis entitled *Jurisdictional Issues Raised by e-Commerce* submitted by *Kathryn Louise Dykstra* in partial fulfillment of the requirements for the degree of *Master of Laws*

Peter Lown

Shannon O'Byrne

Adam Finn

April 14, 2000

Supervisor writes the date that the thesis is approved by committee here

NEW.NEW;G:\dox\kld;877644.WPD;1

Jurisdictional Issues Raised by e-Commerce

Abstract

Internet activity which crosses boundaries between states, provinces and countries raises questions of which courts should take jurisdiction over the complaint or to prosecute the offence and what level of Internet activity constitutes a sufficient connection with the forum for the courts to properly exercise jurisdiction. The answer to this question is important to Canadians doing business on the Internet so they know what country or state laws must be honored, where and in what circumstances they can be subjected to litigation and to know whether a U.S. judgment will be recognized and enforced in a Canadian jurisdiction where their assets are located.

A review of the case law in the U.S. and Canada reveals a trend by the courts to assume both adjudicative and prescriptive jurisdiction based on little more than that the Internet activity results in harmful effects in the forum if the legislation, law or regulation sought to be enforced is one involving a 'protection of the public'. In strictly private disputes, such as a breach of contract action or trademark dispute, the courts generally look first to ensure that the cause of action arises from the Internet activity and, if that connection is found, will address whether there are sufficient additional contacts to justify the assumption of jurisdiction over the defendant and to meet the requirements imposed by the constitutions of the country where the action is brought.

TABLE OF CONTENTS

1. **THE INTERNET** 5

2. **JURISDICTION INVOLVING THE INTERNET** 9

A. General Principles of Jurisdiction Under United States Law 9
B. The United States Experience 14

(a) The Internet and General Jurisdiction 14
(b) The Internet and personal jurisdiction 19

(i) Passive Websites 19
(ii) Passive Website and the "effects test" 24
(iii) Conducting Business over the Internet 26
(iv) Multiple Factors 30

(c) Summary 32

C. General Principles of Jurisdiction under Canadian Law 36

(a) Provincial Rules of Court 36
(b) Real and Substantial Connection 38
(c) Forum Non Conveniens 43

D. Where are the Canadian Courts Headed? 45

(a) Assuming Jurisdiction When the Internet is a Connecting Factor 45
(b) Enforcement of Foreign Judgements 55

3. **INTERACTION WITH CUSTOMERS** 66

A. Sale of Products 66

(a) Commercial Transactions Generally 66
(b) When is a Contract Formed on the Internet? 67
(c) Contract Terms 69
(d) *Uniform Electronic Commerce Act* 71
(e) International Conventions 77
(f) Payment 80
(g) Data Collection – Privacy 80

B. Special Classes of People 90

(a) Consumer Transactions – Advertising 90

C. Special Classes of Products 93

(a) Adjudicatory and prescriptive jurisdiction 93
(b) The Example of Amazon.com 99
(c) Gambling 100
(d) Professional Services 103
(e) Securities 104
(f) Products Carrying Copyright and Trademark Rights 110

(i) Copyright 110
(ii) The Music Industry 117
(iii) Trademarks 125

4. CONCLUSION 125

Electronic commerce ("e-commerce") first emerged in the 1960s on private networks established by large organizations, where electronic data interchange (EDI) and electronic funds transfer (EFT), particularly for banks, dominated development. The competitive advantages gained by large organizations using e-commerce were envied by smaller organizations, but it was not until the development of the Internet[1] that e-commerce began to be available to these firms. Although the Internet was established as a closed network by the U.S. military for security communications, once it became public, it evolved into an open system accessible by people around the world.[2] The explosive growth of the Internet has dramatically changed how people live and communicate, and how firms conduct business.[3]

The growth of e-commerce is paralleled by the growth in its definition. Where once EDI and EFT defined e-commerce, e-commerce now includes any commercial activity conducted over networks linking electronic devices. E-commerce is an economical

---

1 The Internet is a global collection of networks connecting and sharing information through a common set of protocols. It allows computers attached to networks to communicate effectively regardless of make, architecture, operating system or location. Unlike traditional forms of communication, separate networks with separate technologies for voice, data and video transmission are no longer necessary. The Internet can carry these over one simple infrastructure, such as telephone lines, cable lines, or wireless devices.

2 Significant milestones in the development of the Internet, and e-commerce, include: 1969 – Internet/ARPAnet; 1989 – www/html language invented at CERN; 1991 – NSF lifts restrictions on commercial use of Internet; 1993 – Mosaic browser invented at University of Illinois is released to public; 1994 – Netscape releases Navigator browser; 1995 – Dell, Cisco and Amazon begin to aggressively use Internet for commercial transactions.

3 Statistics on e-commerce are widely available. Industry Canada provides these figures for dissemination: Global Internet Commerce – 1998: Business to Business: US $68 billion; Business to Consumer: US $13 billion; Expected Global Internet Commerce – 2003: Business to Business: US $2,960 billion; Business to Consumer: U.S. $240 billion; Canadian Internet Commerce – 1998: Total U.S. $5.5 billion.; Expected Canadian Internet Commerce – 2003: Total US $70 billion (2.1% of global value). Targeted Canadian Internet Commerce – 2003: total US $160 billion. See: http://strategis.ic.gc.ca/virtual_hosts/e-com/using/en/e-comstats.pdf Significant among these statistics is that Canadians rank with Americans as the most Internet-connected people in the G-7.

way of accomplishing tasks that traditionally required a great deal of time and money from businesses. Selling products, invoicing, controlling inventories, and communicating with suppliers and customers are now conducted at incredible speed, with dramatically reduced costs. Given the explosive growth of this form of communication, e-commerce will have increasing significance to the economies of most developed nations. In fact, e-commerce has been described as "the revolution for the 21st century." The revolution will be digital, with information, goods, money and services spinning around the globe with breathtaking new speed and efficiency.

The exponential growth of the Internet as a medium for global commercial activity presents significant challenges to many areas of law including traditional jurisdictional rules. The "borderless" nature of the Internet as an international network of interconnected computers has diminished the relevance of factors such as distance, the physical presence of individuals and territorial controls. A person wishing to conduct business over the Internet through a website has the option of operating from a server in his own office, or 'renting' space from a local Internet service provider (ISP). Alternatively, the e-businessman can arrange for a foreign ISP to carry his website content as the main provider or to operate a mirror site, which would allow those accessing his site from the foreign ISP to obtain access to the content faster.

The website content can be as simple as an advertisement for the product being offered or the company offering the product. More often, the website is used to allow a customer to place an order for almost any product or service imaginable. Although we tend to think of the Internet as primarily providing retail goods and services to the consumer, its

major growth has been in the business to business sector. A car manufacturer, for example, would no longer have a person sitting behind a desk ordering the parts and components required in the course of the assembly process. Instead, the manufacturer would have a software program that 'knows', based on current sales, speed of production and other factors when the company requires delivery of the parts and will order those parts automatically, using electronic agents. The parts supplier's computer, in turn, will automatically order the components that company needs in order to deliver the parts to the car manufacturer within the time specified. You'll note that once the software program is created, no further human intervention is required; the entire transaction being completed by electronic agents. Generally the parties to these types of transactions will negotiate a contract that deals with questions of forum jurisdiction, which jurisdiction's law applies to the contract and whether or not the provisions of an international convention are to apply or be excluded.

Although these business to business transactions do raise some novel legal issues arising from the use of the Internet (can an offer be accepted by an electronic agent?), the more troublesome (and interesting) issues arise from those circumstances where the result of one person's actions on the Internet are immediately available and accessible and can affect persons and entities in different states worldwide. For example, a defamatory statement that is made available in one jurisdiction may affect a person located in another jurisdiction. Use of a trademark registered in Canada to sell a product over the Internet may infringe the trademark of a company selling the same product under the same name in a foreign state. An activity such as gambling may be legal in one state but illegal in another state where the website is accessible. If a doctor gives medical advice over the Internet, must

he be licensed in every state where the advice is accessible? Internet activity that crosses the boundaries between states raises questions of which courts should take jurisdiction over the complaint or to prosecute an offence and, if jurisdiction is assumed, which laws should be applied to the conduct in question.

Presently, the courts of the United States are the vanguard in grappling with these new issues raised by the advent of the Internet, with little Canadian precedent to date. It is expected that the American experience to date will be instructive to Canadian courts faced with the issue of whether to take jurisdiction over a dispute involving the Internet. Specifically, the cases will aid in determining how to apply the concepts of "real and substantial connection" and "properly restrained jurisdiction" as identified by the Supreme Court of Canada in *Morguard Investments Ltd. v. De Savoye*[4] when faced with the inevitable litigation that will occur involving the Internet. It is vital to Canadians doing business on the Internet to know what country or state's laws must be honored, where and in what circumstances they can be subjected to litigation and to know whether a U.S. judgment will be recognized and enforced in a Canadian jurisdiction where their assets are located.

The purpose of this paper is to review and analyze some of the many legal issues raised by e-commerce activities.

---

4 *Morguard Investments Ltd. v. De Savoye* [1990] 3 S.C.R. 1077 at 1103.

1. THE INTERNET

One must understand how the Internet operates to fully appreciate how international law is so profoundly impacted by its presence. As described by one U.S. judge:[5]

> The Internet is not a physical or tangible entity, but rather a giant network which interconnects innumerable smaller groups of linked computer networks. The 'web' is a vast decentralized collection of documents containing text, visual images, and even audio clips. This web is designed to be inherently accessible from every Internet site in the world.

Another U.S. decision characterized the Internet as:[6]

> ...a worldwide network of computers that enables various individuals and organizations to share information. The Internet allows computer users to access millions of Web sites and Web pages. A Web page is a computer data file that can include names, words, messages, pictures, sounds and links to other information.
>
> Every Web page has its own Web site, which is its address, similar to a telephone number or street address. Every Web site on the Internet has an identifier called a 'domain name' ...

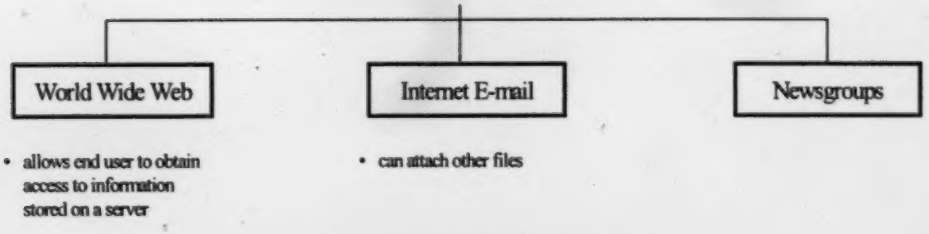
The participants in the process can be grouped into three general categories: the communication providers, the content providers and the end users.

---

5 *Blumenthal v. Drudge*, 992 F.Supp. 44 (D.D.C. at 1998) at 48, footnotes 6 and 7.

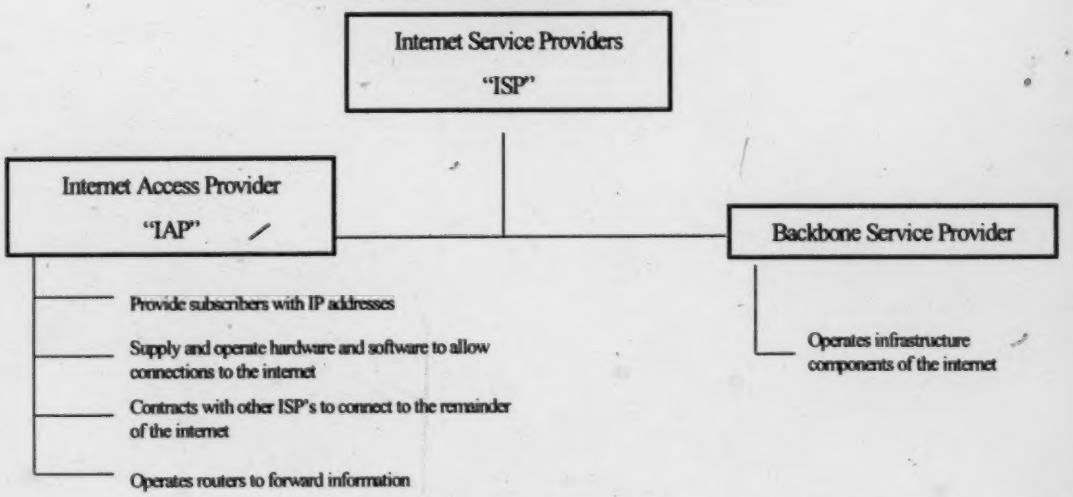
6 *Panavision Intern., L.P. v. Toeppen*, 938 F.Supp. 616 (C.D.Cal.1996) at 1318.

Content Providers

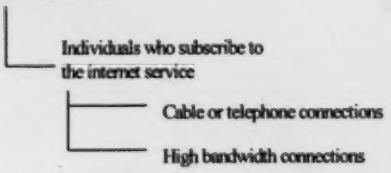


- allows end user to obtain access to information stored on a server
- can attach other files

Communication Services


Internet Service Providers
"ISP"
Internet Access Provider
"IAP"
Backbone Service Provider
Provide subscribers with IP addresses
Supply and operate hardware and software to allow connections to the internet
Contracts with other ISP's to connect to the remainder of the internet
Operates routers to forward information
Operates infrastructure components of the internet

End Users



Each website is stored on a server and the World Wide Web allows an end user to obtain information stored on the server by using a computer program known as a "browser" installed on the user's machine. Provided the user's computer has software that is capable of interpreting the file formats (or language) available, the titles stored in that website can be accessed and downloaded by the end user. The Copyright Board described it very succinctly:[7]

> The essence of what the Internet is and what occurs on it can be stated in a few sentences. It is a telecommunications network. Its purpose is to transmit files containing data, including music as that term is commonly understood. In order for a transmission to occur, the following events must take place. First, the file is incorporated to an Internet-accessible server. Second, upon request and at a time chosen by the recipient, the file is broken down into packets and transmitted from the host server to the recipient's server, via one or more routers. Third, the recipient, usually using a computer, can reconstitute and open the file upon reception or save it to open later; either action involves a reproduction of the file, again as that term is commonly understood.

Does anyone own or control the Internet? Andrew Terrett, in his article "A Lawyer's Introduction to the Internet"[8] describes how many people and firms own and control various small parts of the Internet, but there is no single body that has overall control of activities on the Internet. Terrett describes this fractional ownership as follows:[9]

---

7 Decision of the Copyright Board, *Statement of the Royalties to be Collected for the Performance or the Communication by Telecommunication, in Canada, of Music or Dramatico-Musical Works*, October 27, 1999, at 25.

8 L. Edwards and C. Waelde (eds.), *Law & the Internet: regulating cyberspace* (Oxford: Hart Publishing, 1997).

9 A. Terrett, "A Lawyer's Introduction to the Internet" in L. Edwards and C. Waelde (eds.), *Law & the Internet: regulating cyberspace* (Oxford: Hart Publishing, 1997) at 17.

> Networks within different countries are funded and managed according to local policies and laws. This is both one of the Internet's greatest strengths and one of its main weaknesses. Ownership is distributed between countries and their governments, corporations, universities and telecom utilities. Each individual computer attached to the Internet will be owned by someone, whether a corporation, firm or individual. Telecommunications utilities own the physical wires over which data is transferred. Internet Service Providers (so-called ISP's), telecom utilities or universities will own the data routing equipment. Thus a wide variety of organizations each play a part in owning the Internet.

As a result, there are many differing interest groups that are competing to control the way in which the Internet is used. These include Internet software vendors, software users, free speech advocates, advocates of censorship, governments, information scientists, information providers (both commercial and non-commercial) network administrators and corporations.

The Internet was once the domain of the military and academics. This is clearly no longer the case. Today the Internet is both a personal tool and a powerful business tool utilized for the exchange of electronic messages and documents between a corporation's various branch offices, for advertising, providing information, publishing and online ordering and provision of products and services, to name but a few.

There is wide-spread acceptance of the Internet as a critical tool in marketing one's product to a wide range of consumers. From a computer located anywhere in the world, a user can now type in "amazon.com" and, within a matter of minutes, complete a transaction that will result in books and CDs being delivered to his door within days. Where the product being purchased consists of software or information, the entire transaction can

be initiated and completed on the Internet by downloading the software or information being purchased (for example, the purchase of software or the purchase of a subscription to a magazine or service that is offered on the Internet). The Internet is also being used to trade securities, and numerous brokerage firms are now offering the ability to trade around the clock through the Internet at a lower commission than would otherwise be payable to a traditional broker. Although these trades must still be confirmed by a broker before being submitted to an exchange for execution, it is expected that systems in the future will allow the entire transaction to be completed without any human intervention. This presents both opportunities and problems for regulators trying to protect purchasers from aggressive, and sometimes less than honest, stock promoters.

All of these new business models involving the Internet raise interesting jurisdictional issues. A review of the current state of the law will disclose that in most cases, more than one state may assert that a sufficient component of the transaction occurred in that state or in some manner affected its residents to such an extent to justify that state in assuming jurisdiction over the the complaint. Obviously, as the Internet expands as a mode of business activity, the courts will be faced with adjudicating more and more disputes with the Internet as a significant component in that dispute.

2. JURISDICTION INVOLVING THE INTERNET

A. General Principles of Jurisdiction Under United States Law

One of the basic tenets of international law is that sovereign states have exclusive jurisdiction in their own territory. As a result, states are often hesitant to exercise

jurisdiction over events that may take place in the territory of another sovereign state without good reason.[10] Implicit in the concept of sovereignty is the undisputed right of a state to control both the residents within its jurisdiction and the rights relating to property within that state's jurisdiction. Even when a court has inherent jurisdiction over the parties to a dispute or the subject matter of that dispute, there are still circumstances when the court will decline to take jurisdiction. One example is where the parties to a contract have agreed that another state (or province) will have exclusive jurisdiction in any dispute relating to that contract. Another is where the court finds that the dispute should properly be resolved in another, more appropriate, jurisdiction.

Under U.S. law, a court can assert general jurisdiction over a defendant that is domiciled (or incorporated) within the state, or over a foreign defendant that has engaged in "systematic and continuous" activities in the forum state.[11] These activities must be "so substantial and of such a nature as to justify suit against it on causes of action arising from dealings entirely distinct from those activities".[12] A finding of general jurisdiction over a defendant permits a court to exercise personal jurisdiction (and apply all its laws) over a non-resident defendant regardless of whether the subject matter of the cause of action has any connection to the forum. It will also allow the court to adjudicate any claim against that defendant.

---

10 *Libman v. The Queen* [1985] 2 S.C.R. 178.

11 See generally Gary Born and David Westin, *International Civil Litigation in United States Courts: Commentary & Materials* 2nd ed. (Boston: Kluwer Law and Taxation Publishers, 1992).

12 *International Shoe Co. v. Wash*, 326 U.S. 310 (1945) at 318.

If a U.S. court finds that it does not have general jurisdiction over a defendant, it can still assert limited jurisdiction over the defendant for that specific litigation (a trademark infringement action, for example) if a state's jurisdictional statute confers personal jurisdiction and there is a sufficient connection between the forum, the cause of action and the non-resident defendant. In these circumstances, jurisdiction is taken by the state over non-resident defendants pursuant to what are called "long arm statutes", which provide for "long arm" jurisdiction over, and service of process upon, defendants located outside the forum but who have specified contacts within the state.[13] Although the statutes vary from state to state, there are three basic approaches. Some states use a brief formula to define the circumstances when a court can take jurisdiction. For example the Texas statute provides for jurisdiction over any non-resident defendant who "engages in business" in the state. Some exhaustively list the various circumstances when the court can exercise jurisdiction[14] whereas other long arm statutes permit the courts of that state to exercise personal jurisdiction over non-resident defendants to the constitutional limits of the due process clause of the fourteenth amendment. The fourteenth amendment to the U.S. Constitution[15] limits a state's ability to take jurisdiction when to do so would "offend traditional notions of fair play and substantial justice".[16]

---

13 Gary Born and David Westin, *International Civil Litigation in United States Courts: Commentary & Materials* 2nd ed. (Boston: Kluwer Law and Taxation Publishers, 1992) at 29.

14 Gary Born and David Westin, *International Civil Litigation in United States Courts: Commentary & Materials* 2nd ed. (Boston: Kluwer Law and Taxation Publishers, 1992) at 29.

15 The fourteen amendment to the U.S. Constitution provides that no state shall "deprive any person of life, liberty, or property, without due process of law".

16 *International Shoe Co. v. Wash*, 326 U.S. 310 (1945).

Simply put, the constitutional requirement of "due process" is met, and a court is permitted to exercise personal jurisdiction over a non-resident defendant for forum related activities, when the relationship between the defendant and the forum falls within the "minimum contacts" framework of *International Shoe Co. v. Wash.*[17] There are various tests utilized by the U.S. courts to determine whether such "minimum contacts" exist. One example is the three pronged test as described in *Panavision Intern., L.P. v. Toeppen*:[18]

1. the non-resident defendant must do some act or consummate some transaction with the forum or perform some act by which he *purposefully avails* himself of the privilege of conducting activities in the forum, thereby invoking the benefits and protection of its laws;

2. the claim must be one which *arises out of or results from* the defendant's forum related activities; and

3. the exercise of jurisdiction must be *reasonable*.

"If any one of the three requirements is not satisfied, jurisdiction in the forum would deprive the defendant of due process."[19]

The first prong of the test, namely the "purposeful availment test" differs depending upon the underlying cause of action,[20] however, in general terms, the defendant's

---

17 *International Shoe Co. v. Wash*, 326 U.S. 310 (1945).

18 *Panavision Intern., L.P. v. Toeppen*, 938 F.Supp. 616 (C.D.Cal.1996).

19 *Omeluk v. Langsten, etc.*, 52 F. 3d 267 (9th Cir.1995) at 269.

20 *Panavision Intern.,L.P. v. Toeppen*, 938 F.Supp. 616 (C.D.Cal.1996).

activities must be of a quality and nature that he would anticipate being haled into that forum's court.[21]

The second prong requires that the cause of action arises from or is the result of the transaction or act performed by the defendant within the state.[22] This test "... preserves the requirement that there be some nexus between the cause of action and the defendant's activities in the forum."[23]

The "reasonableness" requirement must be met even though the first two prongs of the test have been met and the defendant has been found to have "minimum contacts" with that state. This third prong requires that the court's exercise of jurisdiction comports with "fair play and substantial justice".[24] In *Burger King Corp. v. Rudzewicz*,[25] the court identified seven factors that must be considered to justify the exercise of jurisdiction:

1. the extent of defendant's purposeful interjection;
2. the burden on the defendant in defending in the forum;
3. the extent of conflict with the sovereignty of the defendant's state;
4. the forum state's interest in adjudicating the dispute;
5. the most efficient judicial resolution of the controversy;

---

21 *Worldwide Volkswagen Corp. v. Woodson*, 444 U.S. 286 (U.S.Okla.1988).

22 *Hansen v. Denckla*, 357 U.S. 235 (1958) at 253.

23 *Shute v. Carnival Cruise Lines*, 897 F. 2d 377 (9th Cir.1990) at 385.

24 *Burger King Corp. v. Rudzewicz*, 471 U.S. 462 (1985) at 477 (quoting *International Shoe Co. v. Wash*, 326 U.S. at 320).

25 *Burger King Corp. v. Rudzewicz*, 471 U.S. 462 (1985) at 477.

6. the importance of the forum to the plaintiff's interest in convenient and effective relief; and

7. the existence of an alternative forum.

Another test used by the courts to claim jurisdiction over a non-resident defendant is the "effects test" of *Calder v. Jones*[26] which focuses on the extent to which the defendant's tortious conduct is aimed at or has effect in the forum state. The "effects doctrine" provides that in tort actions, jurisdiction can be predicated on: (i) intentional actions; (ii) expressly aimed at the forum state; (iii) causing harm, the brunt of which is suffered - and which the defendant knows is likely to be suffered - in the forum's state.[27]

In most cases, and when applying both the 'minimum contacts' test and the 'effects test', the court's focus in the due process analysis is on the defendant's relationship to the forum, and the litigation, rather than the plaintiff's relationship to them.[28] Notwithstanding the court's focus, it is often difficult to discern the precise contours of the due process limits on judicial jurisdiction.

B. **The United States Experience**

(a) **The Internet and General Jurisdiction**

---

26 465 U.S. 783 (1984). In *Calder*, the court chose to exercise jurisdiction on the basis that the defendants knew that California would be the "focal" point of the injuries resulting from their intentional, tortious conduct.

27 *Panavision Intern., L.P. v. Toeppen*, 938 F.Supp. 616 (C.D.Cal.1996) at 621). See also *Intercom, Inc. v. Bell Atlantic Internet Solutions, Inc.*, 2000 WL 262929 (10th Cir.(Okla.)).

28 *Hirsch v. Blue Cross Inc.*, 800 F. 2d 1474 (9th Cir.1986) at 1477.

As indicated above, a U.S. court can assert general jurisdiction over a defendant when that defendant has engaged in "systematic and continuous activities" in the forum state. Such a finding allows the court to assume unlimited jurisdiction over the defendant for any activity, whether or not it is connected with the Internet activity. In cases involving the Internet, when is a defendant "conducting business" sufficient to give the court general jurisdiction? In *IDS Life Ins. Co. v. SunAmerica, Inc.*[29] an action was brought against various defendants for unfair competition, tortious interference with contract, violations of an Illinois statute, violations of the *Copyright Act*, misappropriation of trade secrets and intentional interference with business relationships. One defendant moved to have the action against it dismissed for lack of personal jurisdiction. Under Illinois law, there are two ways that the plaintiff can establish specific (versus general) jurisdiction over a non-resident corporate defendant. First, Illinois' long arm statute permits the exercise of jurisdiction over claims which arise out of the defendant's transaction of business, or commission of a tort, in Illinois. The transaction of business test may be satisfied by an isolated act as long as the plaintiff's claim arises out of that act. Second, the long arm statute also provides that an Illinois court may exercise jurisdiction over a "corporation doing business within the state". No claim had been submitted that SunAmerica had committed tortious acts within Illinois; nor was there any evidence that the plaintiff's claims arose from SunAmerica's commercial activities in Illinois.

---

[29] *IDS Life Ins. Co. v. SunAmerica, Inc.*, 958 F.Supp. 1258 (N.D.Ill.1997).

Therefore, in order to assert jurisdiction over the defendant, the plaintiff had to meet the higher test required for general jurisdiction and to establish that SunAmerica had been carrying on "continuous and systematic" business in Illinois, which can be unrelated to the plaintiff's claims. The plaintiff argued that the court had jurisdiction over the defendant based on a national marketing campaign which included a site on the Internet, advertising in nationally circulated newspapers and magazines, advertising on national television and, in these national advertisements, the provision of a toll free number. The plaintiffs could not demonstrate that SunAmerica had directed any advertisement specifically to Illinois, however the plaintiff was seeking a ruling that any defendant who advertises nationally or on the Internet is subject to the court's jurisdiction in any state where that advertising is circulated or available.

The court disagreed:[30]

> It cannot plausibly be argued that any defendant who advertises nationally could expect to be haled into court in *any* state, for a cause of action that does not relate to the advertisements. Such general advertising is not the type of "purposeful activity" related to the forum that would make the exercise of jurisdiction fair, just or reasonable.

Another case where the plaintiff was arguing that the court should take general jurisdiction over the defendant based on national advertisements was in *McDonough v. Fallon McElligott*.[31] In this case, McDonough, who was a photographer from California, sued the Minnesota advertising agency of Fallon McElligott. McDonough claimed the

---

30 *IDS Life Ins. Co. v. SunAmerica, Inc.*, 958 F.Supp. 1258 (N.D.Ill.1997).

31 *McDonough v. Fallon McElligott*, 40 U.S.P.Q. 2d 1827 (S.D.Cal.1996).

defendants had breached certain copyright provisions by reproducing a photo he had taken of the basketball player, Charles Barkley, in an advertisement which appeared in a national publication. The court confirmed that national publications do not constitute "continuous and substantial contacts" with the forum state, and therefore, the plaintiff had to rely on the defendant's Internet activity to meet the test for jurisdiction.[32]

Fallon McElligott operated a website on the Internet. There was no connection between the copyright infringement and the website (the photo wasn't shown on the website); however, the plaintiff asked the court to take general jurisdiction over Fallon McElligott based on the very existence of the website. The court refused, stating that a website accessed by Californians cannot establish jurisdiction by itself. In considering the issue, the court said that it was not willing to take the step that would allow jurisdiction to exist everywhere there was interaction with that website. To do so would "eviscerate" the personal jurisdiction requirement as it currently exists and, the court went on to say, would be unfair.

Another example is *Weber v. Jolly Hotels*[33] where the New Jersey Federal court dismissed a personal injury suit against an Italian hotel company for lack of personal jurisdiction. The plaintiff had been injured overseas in a hotel operated by the defendant and therefore the only way the court could claim jurisdiction was if the plaintiff could show the defendant conducted business within the state sufficient to allow the court to assume

---

32 For example, see *Gehling v. St. George's Sch. of Medicine, Ltd.*, 773 F.2d 539 (3d Cir.1985).

33 *Weber v. Jolly Hotels, Inc.*, 927 F.Supp. 327 (D.N.J.1997).

jurisdiction over the defendant. The defendant in that case operated a website which offered photographs of hotel rooms, summaries of hotel facilities, information with respect to the hotel rooms and telephone numbers. The plaintiff argued this was sufficient for the court to assume jurisdiction over the defendant in a cause of action entirely distinct from those activities.

The court looked at the existing case law, dividing the cases involving websites into three categories: the first category includes companies that actively do business on the Internet. Such activity would be manifested by a defendant entering into contracts with residents of a foreign jurisdiction that involved a knowing and repeated transmission of computer files over the Internet. The second category includes those situations where a user can exchange information with the host computer. Whether or not a court should take jurisdiction in these circumstances depends on the level of interactivity and the commercial nature of the exchange of information that occurs on that website. The third category includes what the court describes as "passive sites" which merely provide information or advertising. On the facts before it, the court held that the defendant was merely operating a passive site and that to take jurisdiction of disputes in this latter category would be inappropriate:[34]

> ... a finding of jurisdiction ... based on an Internet website would mean that there would be nationwide (indeed, worldwide) personal jurisdiction over anyone and everyone who establishes an Internet website. Such nationwide jurisdiction is not consistent with traditional personal jurisdiction case law....

---

[34] *Weber v. Jolly Hotels, Inc.*, 927 F.Supp. 327 (D.N.J.1997).

Patriot Systems, Inc. v. C-cubed Corporation[35] is a similar case where the defendant operated a website but there was no connection between the website and the cause of action. The court declined jurisdiction in this instance as well.

From the foregoing cases it would seem reasonable to conclude that the existence of a website, without more, is insufficient to give the court general jurisdiction over a defendant in those circumstances where the Internet activity is unrelated to the cause of action.

(b) **The Internet and personal jurisdiction**

Typically, however, in most cases involving the Internet, the plaintiff is only asking the court to assume jurisdiction over the defendant for specific litigation which arises out of or results from the defendant's forum related activities. The test for such personal jurisdiction is therefore much lower. As indicated previously, the tests used by the courts to assert personal jurisdiction in these circumstances (assuming the long arm statute permits jurisdiction) are the "minimum contacts" test and the "effects doctrine".

(i) **Passive Websites**

The decision in *Inset Systems Inc. v. Instruction Set, Inc.*[36] illustrates how low the threshold level of activity can be to meet the required "minimum contacts" for personal jurisdiction over a given action. In *Inset Systems*, the plaintiff sued in its home state of Massachusetts for an injunction in a trademark infringement action based on the defendant's

---

35 *Patriot Systems, Inc. v. C-cubed Corporation*, (1998) WL 668625 (D.Utah).

36 *Inset Systems, Inc. v. Instruction Set, Inc.*, 937 F.Supp. 161 (D.Conn.1996).

use of the plaintiff's name as its domain name. The defendant was operating a website under the name "Inset.com" that contained an advertisement and a toll free number - what would be described in *Weber Hotels* as a "passive site". The evidence focused on by the court included the fact that the defendant directed its advertising to every state, through the Internet and through provision of a toll free number, and the fact that over 10,000 people were connected to the Internet in Massachusetts and therefore had access to the defendant's website. Based on these factors, the court stated that the defendant purposely availed itself of the privilege of doing business with Massachusetts and therefore met the "minimum contacts" required for the court to assert its jurisdiction over the action.

Inset Systems has been described by one court as the "outer limits",[37] however, there was a similar result in the later case of *Telco Communications v. An Apple A Day*,[38] a defamation action where the defendant had done little more (other than posting a defamatory press release on its website) and the court found that the website, together with a phone number and the "active solicitation" on that website was sufficient to meet the "minimum contacts" test required by *International Shoe*. In both *Inset* and *Telco Communications*, there was a connection between the website and the cause of action and therefore the second prong of the test enunciated in *Panavision* had been met. The question was therefore whether the

---

37 *Zippo Mfg. Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119 (W.D.Pa.1997) at 1125.

38 *Telco Communications v. An Apple A Day*, 977 F.Supp 404 (E.D.Va.1997).

defendant's actions met the "purposeful availment" test, and in both *Inset* and *Telco Communications* a website with a phone number was sufficient to meet that test.[39]

In the case of *Bensusan Restaurant Corp. v. King*[40] the court came to a different conclusion because it found that the allegedly infringing activity of the website at issue was not aimed at New York residents. The plaintiff in this case was the creator of a jazz club in New York city known as "The Blue Note" who also owned a federally registered trademark for the same name. The defendant, King, is an individual who owns and operates a small club in Columbia, Missouri also called The Blue Note. The defendant operated a website which contained general information about the club in Missouri as well as a calendar of events and ticketing information. The site included a telephone number for charge-by-phone ticket orders. King moved to dismiss the trademark infringement action for lack of personal jurisdiction.

New York's long arm statute allows the court to take personal jurisdiction over any non-resident who "commits a tortious act within the state" as long as the cause of action asserted arises from the tortious act. In determining whether this portion of the statute had been met, the court followed the decision of the United States Court of Appeals for the Second Circuit[41] where it was held that trademark infringement occurs "where the passing

---

39 See, however, *GTE New Media v. Bell South*, D.C. Cir. No. 99 - 7097, January 11, 2000, where the court said that access to a website in the jurisdiction, plus telephone contact with residents was insufficient for personal jurisdiction. See also *Blackburn v. Walker Oriental Rug Galleries, Inc.*, 999 F. Supp. 636 (E.D.Pa. 1998).

40 *Bensusan Restaurant Corp. v. King*, 40 U.S.P.Q. 2d 1519 (1996).

41 *Bensusan Restaurant Corp. v. King*, 40 U.S.P.Q. 2d 1519 (1996) at 1522.

off occurs, i.e., where the deceived customer buys the defendant's product in the belief that he is buying the plaintiff's." The issue, as posed by the court, was whether "the creation of a website, which exists either in Missouri or cyberspace - i.e., anywhere the Internet exists - with a telephone number to order the allegedly infringing product, is an offer to sell the product in New York."[42] Under this test, any act of infringement would have occurred in Missouri as the only way to attend a show at the defendant's club would be to contact the box office in Missouri and to pick up the tickets in Missouri because the defendant did not mail or otherwise transmit tickets to the user. Accordingly, the court would not assert jurisdiction under this section of the long arm statute.

A second section of the long arm statute pleaded by the plaintiffs was one which allows a court to exercise personal jurisdiction over any non-resident for a tortious act committed outside the state that causes injury in the state if the non-resident "expects or should reasonably expect the act to have consequences in the state and derives substantial revenue from interstate or international commerce".[43] Firstly, the court found that injury was not caused to the plaintiff in New York as the website had virtually no effect on New York residents. While it is true that the website could be accessed in New York, it was essentially aimed at residents of Missouri and neither caused confusion in New York nor was aimed at New York residents. It was found that the defendant made no effort to serve the market in

---

42 *Bensusan Restaurant Corp. v. King*, 40 U.S.P.Q. 2d 1519 (1996) at 1522.

43 *Bensusan Restaurant Corp. v. King*, 40 U.S.P.Q. 2d 1519 (1996) at 1522.

New York, nor did it derive substantial revenue from out of state customers. In fact, it received very little revenue from out of state customers.

Even if jurisdiction could be established under New York's long arm statutes, the court found that asserting jurisdiction over King would offend the "due process" clause. It was held that creation of a website, without more, is not an act purposefully directed towards the state. There was no suggestion that King had any other contacts with or presence in New York other than the website. The court refused to take jurisdiction.

The District Court in New York, in a later case, came to the same conclusion. In *Hearst Corporation v. Goldberger*,[44] Hearst, the owner and publisher of Esquire magazine, brought a trademark infringement action against Goldberger who had established an Internet domain name and website under the name "esq.wire.com.". The website was offering law office infrastructure network services for attorneys which was totally unrelated to the products offered by the plaintiff. The court found that, while Goldberger had operated a website, it had not sold any products or services. Furthermore, the defendant had not targeted the New York market, per se, and therefore the court considered the website as analogous to a publication in a national magazine and such advertising would not constitute sufficient contacts with New York to provide the court with personal jurisdiction over Goldberger. As a matter of policy, the court, in that instance, was not prepared to extend jurisdiction everywhere there is access to a website.

---

[44] *Hearst Corporation v. Goldberger*, (1997) WL 97097 (S.D.N.Y.).

Likewise, in *Barrett v. The Catacombs Press*,[45] the court refused to follow *Inset Systems* and in fact went even further in holding that the posting of defamatory messages to various national listserves, or news discussion groups, with links back to the defendant's passive website was insufficient to elevate the activity beyond that of a passive website for jurisdiction purposes. Like *Bensusan* and *Hearst Corporation*, the defendant never targeted or solicited residents of the forum.

(ii) **Passive Website and the "effects test"**

The weight of the case law suggests that something more than a website advertisement available to anyone who has access to the Internet is required for personal jurisdiction. The "something more" may be the intention of the defendant, which is relevant when applying the "effects test". This test was applied by the court in a "cybersquatter" case in California.

Panavision Intern., L.P. v. Toeppen[46] was an action based on a dispute between the holder of a registered trademark and the holder of a registered domain name. Panavision, a California business, brought a trademark infringement and dilution action against an Illinois resident who registered the Panavision trademark as a domain name for his Internet website. After registering the "panavision.com" domain name, the defendant established a website displaying aerial views of Pana, Illinois. At no time did the defendant use the panavision.com name in connection with the sale of any goods or services.[47] When

---

45 *Barrett v. The Catacombs Press*, No. 99-736 (D.C.E.D. Pa. April 12, 1999).

46 *Panavision Intern., L.P. v. Toeppen*, 938 F.Supp. 616 (C.D.Cal.1996).

47 *Panavision Intern., L.P. v. Toeppen*, 938 F.Supp. 616 (C.D.Cal.1996) at 619.

Panavision went to register its trademark as a domain name, Network Solutions, Inc. which registers Internet domain names, refused to allow the registration. The plaintiff asserted that the sole purpose for the defendant registering the domain name was to extort money from Panavision and in fact Toeppen had demanded $13,000 from the plaintiff to discontinue use of the domain name.

The court found that it did not have general jurisdiction over the defendant in that he was not a resident of California and his activities in California were not substantial, systematic or continuous. In fact, the only activity that the defendant undertook was to operate the website showing the view of the town of Pana under the domain name of panavision.com. Notwithstanding such minimal contacts with the state, the court took jurisdiction under the "effects doctrine". Applying this doctrine, the defendant was held to be subject to personal jurisdiction in California on the basis that he had registered Panavision's trademark as a domain name with the knowledge that the name belonged to Panavision and with the intent to interfere with Panavision's business.[48] Further, the court determined that jurisdiction was proper because the defendant's out of state contact was intended to, and did, result in harmful effects in California. The court, referring to other Internet cases where the existence of a website was insufficient to confer jurisdiction, stated that those cases were not analogous to the case before the court:[49]

---

[48] *Panavision Intern., L.P. v. Toeppen*, 938 F.Supp. 616 (C.D.Cal.1996) at 621.

[49] *Panavision Intern., L.P. v. Toeppen*, 938 F.Supp. 616 (C.D.Cal.1996) at 622.

> The issue in those cases was whether contacts with the forum state via the Internet ... were sufficient to confer jurisdiction.
>
> Although at first blush the cases seem similar to the case at bar the semblance is superficial only. In each of those cases, the parties had legitimate business and legitimate legal disputes. Here, however, Toeppen [the defendant] is not conducting a business but is, according to Panavision, running a scam directed at California.

In those cases where "cybersquatting" (i.e. the defendant has obtained a domain name containing the plaintiff's trademark and is trying to sell the domain name to the plaintiff) is an issue, the courts, as in *Panavision* are loathe to give the defendant any advantage. If the "extortion" aspect is absent, the courts tend to apply the "minimum contacts" test in a more objective manner.[50]

(iii) **Conducting Business over the Internet**

The category of cases where the courts have little difficulty exercising jurisdiction are those where the Internet activity involves the conduct of business over the Internet including online contracts with residents of the forum or substantial inter-activity of a commercial nature with the website. One such example is the Ohio case of *CompuServe, Inc. v. Patterson*.[51]

CompuServe, located in Ohio, was appealing a lower court's finding that the defendant had insufficient contacts with Ohio to allow the court to take jurisdiction. Patterson, a resident of Texas, was claiming that CompuServe had infringed its trademark

---

50 See, for example, *Hearst Corporation v. Goldberger*, (1997) WL 97097 (S.D.N.Y.).

51 *CompuServe, Inc. v. Patterson*, 89 F. 3d 1257 (6th Cir. 1996).

and CompuServe was seeking a declaratory judgment that it had not. The court found that Patterson had knowingly made an effort and had purposefully contracted to market a product in other states with the Ohio based CompuServe operating as his distribution centre. In particular, the court found the defendant had a "substantial connection" with the forum state as more than a purchaser of CompuServe's services: Patterson transmitted his software from Texas to CompuServe's system in Ohio; others gained access to Patterson's software via that system; and Patterson advertised and sold his product through that system.[52] The court ultimately determined there was a business relationship between Patterson and CompuServe that had extended for some three years and therefore Patterson should have reasonably foreseen that carrying on this on-going marketing relationship with CompuServe would have consequences in Ohio.

The court had little difficulty taking jurisdiction as a result of the defendant's commercial activity with the forum state in *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*,[53] an action involving a dispute between the holder of a trademark and the holder of a domain name. Zippo Manufacturing ("Zippo") commenced a trademark infringement action against Zippo Dot Com ("Dot Com") in Pennsylvania, where Zippo manufactures tobacco lighters under the name "Zippo". Dot Com is a California company which operates an Internet website and an Internet news service and has the exclusive right to use the domain names "Zippo.com", "Zippo.net" and "Zippo-news.com" on the Internet. The question being

---

52 *CompuServe, Inc. v. Patterson*, 89 F. 3d 1257 (6th Cir.1996).

53 *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*, 952 F.Supp. 1119 (W.D.Pa.1997).

dealt with by the Pennsylvania court was whether or not it had jurisdiction to hear the dispute.

The court, after reviewing the recent cases, stated that "the likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet".[54] The court went on to describe a "sliding scale" where at the one end of the spectrum are defendants who enter contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files on the Internet. The court felt that in these circumstances personal jurisdiction is proper and cited the case of *CompuServe Inc. v. Patterson*.[55]

At the opposite end of the scale are passive websites that do little more than make information available to those persons who are interested, and in these circumstances, according to the court, it is not proper for the court to exercise personal jurisdiction. In circumstances where a user is able to exchange information with the host computer, the courts must examine the level of interactivity and the commercial nature of the exchange of information that occurs on a website to determine if such activity is sufficient to assume jurisdiction. In this instance, the court held that the defendant had gone beyond the level of an interactive website and was exchanging information with Pennsylvania residents. Dot Com had contracted with approximately 3,000 individuals and 7 Internet access providers

---

54 *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*, 952 F.Supp. 1119 (W.D.Pa.1997) at 1124.

55 *CompuServe, Inc. v. Patterson*, 89 F.3d 1257 (6th Cir.1996).

in Pennsylvania and the purpose of these transactions was to sell to the individuals electronic messages that could be downloaded onto their individual computers. This was a clear case of "doing business over the Internet" in line with *CompuServe*. In addition, the court held that the cause of action arose out of Dot Com's forum related conduct, as the cause of action for a trademark infringement occurs where the passing off occurs. In the view of the court, all prongs of the minimum contacts test had been met.[56]

A further example in which an interactive website coupled with active solicitation of business on that site is the case of *Maritz, Inc. v. Cybergold, Inc.*[57] This matter involved a dispute between holders of two different trademarks. The plaintiff, Maritz, owned the trademark for the name "Goldmail" in connection with an Internet mail service who sued the user of the "Cybergold" mark in connection with a similar service for trademark infringement. The action was commenced in Missouri and the server, from which the defendant's website was operated, was located in California. The defendant in this case operated a website to promote its upcoming Internet service which would assign users an electronic mailbox and then forward advertisements for products and services that matched the user's interests to those electronic mailboxes. Cybergold sought to provide users with incentives for viewing the advertisements and to charge advertisers for access to the users on its mailing list. Cybergold's actual mailbox service was not yet in operation. The plaintiff

---

[56] *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*, 952 F.Supp. 1119 (W.D.Pa.1997) at 1127. See also *Mink v. AAAA Development* LLC, 190 F.3d 333, 1999 Corpr. L. Dec. P 27, 954, 52 U.S.P.Q. 2d 1218 (5th Cir. Tex.) Sept.17, 1999 (No. 98-20770).

[57] *Maritz, Inc. v. Cybergold, Inc.*, 947 F.Supp. 1228 (E.D.Mo.1996).

argued that Cybergold was actively soliciting advertising customers from Missouri whereas Cybergold argued that its site was merely a "passive website" in the nature of *Bensusan*.

The courts, having to determine whether the defendant's solicitations constituted minimum contacts with Missouri, held that Cybergold's contacts with residents of the forum were more interactive than a "passive website". In fact, Cybergold had transmitted advertising e-mails to Missouri residents approximately 131 times. This interactivity with Missouri residents was sufficient to give the court jurisdiction.

(iv) **Multiple Factors**

An additional category of cases are difficult to classify because non-Internet contacts factored into the court's decision as to whether the exercise of personal jurisdiction was proper. *Digital Equipment Corp.*[58] is one example where the "minimum contacts" test was satisfied by the defendant's Internet activity plus additional factors.

The defendant, Altavista, entered into a contract with Digital that contained a choice of law clause requiring the contract to be interpreted under the laws of Massachusetts, the jurisdiction in which the plaintiff carried on business and in which the action for breach of a trademark licensing agreement and trademark infringement action was commenced. In addition, it was found that Altavista was soliciting business and product sales through its website, including business in Massachusetts, and had made three sales to Massachusetts residents. It was this very conduct which gave rise to the cause of action by

---

[58] *Digital Equip. Corp. v. Altavista Tech., Inc.*, 960 F.Supp. 456 (D.Mass.1997).

Digital, which claimed that Altavista was infringing Digital's trademark and causing considerable confusion in Massachusetts as a result.

The operation of this website infringed the plaintiff's trademark and breached the contract between the parties and therefore created the "minimum contacts" necessary to exercise jurisdiction. Similar to other cases, the court drew an analogy between a website and national publications: on a website, potentially innumerable "copies" can be (and are) regularly "distributed" wherever there is access to the world wide web.[59] In *Digital*, however, the court stated that such publication would be sufficient if it gave rise to the very conduct which comprises the cause of action, which would suggest, in a liberal interpretation, cases involving defamation on the Internet or trademark infringement would give every state jurisdiction.

In *Heroes*,[60] it was found that a webpage together with an advertisement in a local paper soliciting contributions to the defendant, Heroes Foundation, was sufficient to trigger jurisdiction.

In *Blumenthal v. Drudge*[61] the defendant operated a website with defamatory material, but also made trips to the District of Columbia to promote his website and made various contacts with residents of the District via e-mail, telephone and mail to obtain gossip for his column. The court took jurisdiction.

---

59 *Digital Equip. Corp. v. Altavista Tech., Inc.* 960 F.Supp. 456 (D.Mass.1997) at 470.

60 *Heros, Inc. v. Heroes Foundation*, 958 F.Supp. 1 (D.D.C.1996).

61 *Blumenthal v. Drudge*, 992 F.Supp. 44 (D.D.C. 1998).

Where the court finds that there is a business relationship between the parties they have little hesitation in asserting jurisdiction, particularly where that relationship results in a contract.[62] This holds true even where the plaintiff's claim does not arise directly from the contractual relationship.[63] For example, in *Edias Software Intern. v. Basis Intern. Ltd.*, it was held that a contract and a long standing relationship between the parties was sufficient to trigger jurisdiction for defamatory statements made by the defendant via e-mail and through the web page. The contract itself obligated the defendant to distribute the plaintiff's products outside of Arizona, the forum state, and that New Mexico law would apply to the contract. The only connection in the contract with Arizona was that it was the plaintiff's principal place of business and it was provided that the defendants were to mail their invoices to that address. However, the business relationship between the parties that involved communication by e-mail, fax and telephone with the plaintiff in Arizona together with the defendant's website, constituted the "minimum contacts" required to take jurisdiction.

(c) **Summary**

An analysis of the jurisprudence in the U.S. does not reflect complete consistency in the application of the traditional jurisdictional rules. It appears that both the nature of the claim together with the connection between the activity on the Internet and the cause of action are critical in a court's determination of whether a defendant, through its

---

62 *Hall v. LaRonde*, 66 Cal. Rptr. 2d 399 (Cal.App.2Dist.1997).

63 *Edias Software Intern. v. Basis Intern. Ltd.*, 947 F.Supp. 413 (D.Ariz.1996).

activities on the Internet, has made sufficient contacts with the forum to confer specific jurisdiction on that state's courts. If the cause of action arises from the very existence of a website (defamation or trademark infringement, for example) the mere ability to access a passive website may be sufficient to give rise to jurisdiction, although it is likely that in trademark infringement actions, other than those dealing with "cybersquatters", some other interactive factors, such as solicitation in the jurisdiction may be required. Notwithstanding that the second prong of the test described in *Panavision*[64] requires that the cause of action arises out of the defendant's forum related activities, the Court will also look at factors unrelated to the defendant's Internet activity to see if minimum contacts exist. Accordingly, the greater the level of interaction between the defendant and either the residents of the state or the plaintiff, the greater the likelihood of the courts assuming jurisdiction.

If there is no connection between the activity on the website and the claim, and there are no "other factors", a much higher level of interactivity is required in order for the court to assert general jurisdiction over the defendant - the court must be satisfied that the defendant's activities are "continuous and systematic" in that state.

The following chart of cases categorizes the major cause of action, the level of Internet activity, whether or not the Internet activity gave rise to the cause of action and the court's determination on the issue of jurisdiction.

---

[64] *Panavision Intern., L.P. v. Toeppen*, 938 F.Supp. 616 (C.D.Cal.1988) at 1318.

Case	Cause of Action	Internet Factors	Connection Between Cause of Action and Internet Activity	Jurisdiction
Bensusan Restaurant Corp. v. King	tort (trademark)	passive website not "aimed at" New York	Yes*	No
Panavision Intern., L.P. v. Toeppen	tort (trademark)	passive website "cybersquatter"	Yes	Yes
IDS Life Ins. Co. v. SunAmerica, Inc.	tort (trademark)	passive website	No	No
Inset Systems Inc. v. Instruction Set, Inc.	tort (trademark)	passive website	Yes	Yes
Patriot Systems, Inc. v. C-cubed Corporation	tort (trademark)	passive website	No	No
Weber v. Jolly Hotels, Inc.	tort (trademark)	passive website	No	No
Barrett v. The Catacombs Press	tort (defamation)	passive website not "aimed at" Pennsylvania and posting on Internet discussion group	Yes	No
McDonough v. Fallon McElligot Inc.	tort (trademark)	low level interactive	No	No
Hearst Corporation v. Goldberger	tort (trademark)	low level interactive	Yes*	No
Blumenthal v. Drudge	tort (defamation)	website/active solicitation	yes	yes
Heroes, Inc. v. Heroes Foundation	tort (trademark)	active solicitation on website "newspaper ads"	Yes	Yes
Digital Equip. Corp. v. Altavista Tech., Inc.	contract and tort	active solicitation contract with plaintiff	Yes	Yes
Maritz, Inc. v. Cybergold, Inc.	tort (trademark)	active solicitation	Yes	Yes
CompuServe, Inc. v. Patterson	tort (trademark)	active solicitation	Yes	Yes

Case	Cause of Action	Internet Factors	Connection Between Cause of Action and Internet Activity	Jurisdiction
Zippo Mfg. Co. v. Zippo Dot Com, Inc.	tort (trademark)	interactive; contracts with residents	Yes	Yes
Edias Software Intern. v. Basis Intern. Ltd.	contract	business relationship	No	Yes

* The court did not focus on the connection, but it was in fact the website activity that was the offensive conduct.

From a review of the cases to date in the U.S., it would appear that the courts will exercise jurisdiction, where there is a connection between the Internet activity and the cause of action, in the following circumstances:

(a) the defendant's website is located within the jurisdiction or the defendant operates a business in the forum;

(b) the plaintiff and the defendant have a business relationship expressed in a contract or developed through other means;

(c) the defendant actively solicits business in the state through the Internet and in fact sells to or conducts commercial transactions with residents of the forum, other than the defendant;

(d) there is repeated interaction between the defendant and residents of the forum state;

(e) even though the defendant operates a passive website, and does not solicit business within the jurisdiction, the court will exercise jurisdiction in a trademark infringement action when the defendant uses a domain name that appears to infringe on the plaintiff's trademark but only if the defendant is attempting to extract money from the plaintiff in exchange for the right to use that domain name ("cybersquatters").

If the harm is caused to the plaintiff by the mere operation of the website (as in a trademark infringement), the court will likely decline jurisdiction, unless there are other

factors present, such as a contract or other business relationship between the parties or the defendant deliberately targets the forum. The courts often state that in these circumstances, the defendant is put on adequate notice that his actions may result in being haled into court in a state where he is doing business.

The implication of a ruling like *Inset*, while considerable, appears to be losing favour. It is likely that the mere presence of a website, the contents of which are alleged to cause harm, will no longer be sufficient to give a court jurisdiction anywhere the site can be accessed.

C. General Principles of Jurisdiction under Canadian Law

What can one expect from Canadian courts faced with these same issues? Although Canada's constitution does not have a "due process" limitation like the United States, there are limitations on a province's ability to extend its jurisdiction arising from the division of powers between the provinces and the federal government.

(a) Provincial Rules of Court

As a starting point one must examine the basis for a court's assumption of jurisdiction in the provinces and, to illustrate by way of example, reference will be made to the legislative basis in Alberta. As in the U.S., where an action is brought in Alberta, the conflict of law rules will be applied to resolve the jurisdictional question before the court. In doing so, the court will apply its own procedural rules to determine whether or not the court has jurisdiction to hear the matter and whether the court will assume jurisdiction over

the defendant. The *Court of Queen's Bench Act*[65] allows an Alberta court to take jurisdiction over all matters except those specifically granted to another court[66] by statute. Within that scope, the *Alberta Rules of Court*[67] permit a court to assume jurisdiction over all persons and matters within its territorial jurisdiction including persons available to be served within the province. In addition, the court is permitted to extend that jurisdiction beyond residents of Alberta and beyond property located within Alberta in those circumstances set out in Rule 30.[68] Pursuant to this Rule, which is a code defining the court's jurisdiction, provision is made for serving a defendant outside the province whenever:

(a) the subject matter of the action is land situated within Alberta or where the contract, obligation, liability, deed or act sought to be construed, rectified, set aside or enforced directly affects land situated within Alberta;

(b) relief is sought against a person ordinarily domiciled or resident within Alberta;

(c) the proceeding is to enforce, rescind, resolve, annul or otherwise affect a contract or to recover damages or to obtain any other relief in respect of the breach of a contract being (in any case) a contract:

(i) made within Alberta;

---

65 *Court of Queen's Bench Act* RSA 1980, c.C-29.

66 For example, when jurisdiction is given to a federal court or a provincial court.

67 A.R. 390/68; 338/83.

68 In most provinces there is a rule similar to Rule 30. In Ontario, see Rules 17.02 and 17.03 of the Ontario Rules of Civil Procedure and in British Columbia, see Rule 13 of the British Columbia Rules of Court.

(ii) made by or through an agent trading or residing within Alberta on behalf of a principal out of Alberta;

(iii) which is by its terms, or by implication governed by Alberta law or for which the parties thereto agree that the courts of Alberta shall have jurisdiction to entertain any action in respect of the contract;

(d) the action is in respect of a breach committed within Alberta of a contract made within or outside of Alberta;

(e) the action is founded on a tort committed within Alberta;

(f) in the action, an injunction is sought ordering a defendant to do or refrain from doing anything within Alberta (whether or not damages are also claimed in respect of a failure to do or the doing of that thing).

There are other grounds for a court assuming jurisdiction, but the foregoing comprise the major categories and are similar in most common law provinces.[69] Canadian courts, like those in the U.S., have the ability to extend their reach far beyond the territorial limits of the state, or in this case, the provinces. Prima facie, under Rule 30, an Alberta court could assume jurisdiction in every instance where a U.S. court assumed jurisdiction as described in the hereinbefore mentioned cases.

(b) **Real and Substantial Connection**

Canadian courts have recently recognized, like their American counterparts, that restraint must be exercised when assuming jurisdiction beyond their territorial borders.

---

[69] There are differences in methods, but not the grounds.

In *Morguard Investments Ltd. v. De Savoye*[70] the Supreme Court of Canada discussed the concept of "properly restrained jurisdiction" and the requirement for a "real and substantial connection" with the province assuming jurisdiction. In *Morguard*, the plaintiffs, Credit Foncier Trustco and Morguard Investments Ltd. had obtained a judgment in Alberta against a British Columbia resident for foreclosure and for the deficiency between the value of the property and the amount owing under the mortgages. The question before the court was whether or not the Alberta judgment should be enforced by a British Columbia court.[71] LaForest reviewed the objectives of private international law and confirmed that a modern system of private international law must be based upon principles of order and fairness, principles that ensure security of transactions with justice. He went on to quote Hessel E. Yntema, "*The Objectives of Private International Law*" (1957), 35 Can.Bar.Rev. 721, at p. 741:[72]

> In a highly integrated world economy, politically organized in a diversity of more or less autonomous legal systems, the function of conflict rules is to select, interpret and apply in each case the particular local law that will best promote suitable conditions of interstate and international commerce, or, in other words, to mediate in the questions arising from such commerce in the application of the local laws.

---

70 *Morguard Investments Ltd. v. De Savoye* [1990] 3 S.C.R. 1077.

71 Prior to *Morguard*, where a defendant was served outside the jurisdiction of the court adjudicating the matter, the ensuing judgment would only be enforced by a sister province if the defendant had either consented to or attorned to the jurisdiction of that original court. In *Morguard*, the court held this approach to be inconsistent with the federal structure of our constitution. Instead, the court in the sister province should look at the contacts between the province that took original jurisdiction, the defendant and the subject matter of the action.

72 *Morguard Investments Ltd. v. De Savoye* [1990] 3 S.C.R. 1077 at Q.L., p. 11.

Although this statement was made by its author in 1957 and was quoted by LaForest in 1990, it remains pertinent and relevant when dealing with questions related to the issues raised by commerce in cyberspace.

LaForest stated that where the courts in another province or territory have appropriately exercised jurisdiction in the action, that court's judgment should be recognized. In addressing the question of whether the Alberta courts properly assumed jurisdiction over a non-resident, LaForest said:[73]

> ... the principles of order and fairness should obtain in this area of the law. Both order and justice militate in favour of the security of transactions. It seems anarchic and unfair that a person should be able to avoid legal obligations arising in one province simply by moving to another province. Why should a Plaintiff be compelled to bring an action in the province where a Defendant now resides, whatever the inconvenience and costs this may bring, and whatever degree of connection the relevant transaction may have with another province?
>
> These concerns, however, must be weighed against fairness to the Defendant. I noted earlier that the taking of jurisdiction by a court in one province and its recognition in another must be reviewed as correlatives, and I added that recognition in other provinces should be defended on the fact that the court giving judgment "properly" or "appropriately" exercised jurisdiction. It may meet the demands of order and fairness to recognize a judgment given in a jurisdiction that had the greatest or at least significant contacts with the subject matter of the action. But it hardly accords with principles of order and fairness to permit a person to sue another in any jurisdiction, without regard to the contact that jurisdiction may have to the Defendant or the subject matter of the suit; see Joost Blom, "*Conflict of Laws - Enforcement of Extra-provincial Default Judgment - Reciprocity of Jurisdiction:*

---

[73] *Morguard Investments Ltd. v. De Savoye* [1990] 3 S.C.R. 1077 at Q.L., p. 14.

> *Morguard Investments Ltd. v. De Savoye*" (1989), 68 Can.Bar.Rev.359 at p.360. Thus, fairness to the Defendant requires that the judgment be issued by a court acting through fair process and with properly restrained jurisdiction.

If a court bases its jurisdiction on traditional grounds of residence, or by virtue of an agreement to give the court jurisdiction, then no injustice results. In other circumstances, however, LaForest recognized that the rules for service *ex juris* in all the provinces are broad and therefore there must be some limits placed on a province's ability to exercise jurisdiction over persons residing outside that province.[74] He agreed with the approach of the House of Lords in *Indyka v. Indyka*[75] which required a real and substantial connection between the defendant and the country or territory claiming to exercise jurisdiction. If such a real and substantial connection exists, then it is "inherently reasonable" for the action to be brought in that particular jurisdiction.

In *Hunt v. T & N. plc*[76] the Supreme Court of Canada adopted the principles expounded in *Morguard* and confirmed that, for constitutional reasons, there must be a real and substantial connection between the defendant and the forum province such that it is reasonable for the courts to infer that the defendant voluntarily submitted itself to the risk of jurisdiction in its courts.[77] Failing such a connection, the proceeding may be challenged on the constitutional ground that the province has exceeded its power to legislate under Section

---

74 *Morguard Investments Ltd. v. De Savoye* [1990] 3 S.C.R. 1077 at Q.L., p. 15.

75 *Indyka v. Indyka*, [1969] 1 A.C. 33.

76 *Hunt v. T & N plc* [1993] 4 S.C.R. 289.

77 *Canadian Conflict of Laws*, 4th ed. (Vancouver: Butterworths, 1997), J.G. Castel.

92(13) of the *Constitution Act*, 1867. A province's ability to govern a person by legislation passed pursuant to Section 92(13) requires some contacts by that person with the province.

It is difficult to predict with certainty what factors would establish a real and substantial connection for the purposes of establishing jurisdiction. As stated by Castel:[78]

> A real and substantial connection with the original forum, province or territory can be anything. It depends upon the circumstances, provided the connection used by the court is not unfair to the defendant.

In *Moses v. North Shore Boat Builders* (1992), 68 B.C.L.R. (2d) 394 (S.C.); affirmed (1993), 83 B.C.L.R. (2d) 177 (C.A.), where the plaintiff sued in British Columbia to enforce a judgment he had obtained in Alaska for breach of warranty by the B.C. manufacturer and vendor of a fish boat, Justice Cumming, for the court, said at 189:

> The courts of British Columbia consider a wide variety of factors when deciding whether or not the action has a real and substantial connection to British Columbia. Common considerations include: the place the cause of action arose; the respective residences of the parties; whether the defendant conducted business or had other dealings in British Columbia, and other similar "connecting factors".

---

[78] *Canadian Conflict of Laws*, 4th ed. (Vancouver: Butterworths, 1997), J.G. Castel at 281.

The courts in Canada have also applied the test in *Morguard* to judgments rendered outside Canada and sought to be enforced in Canada.[79] As reasoned by the B.C. Court of Appeal in *Moses v. North Shore Boat Builders*:[80]

> In summary, the judgment of the Supreme Court of Canada in *Morguard, supra*, offers substantial reasons to extend the real and substantial connection test to the enforcement of foreign judgments...Modern rules of international law must accommodate the flow of wealth, skills and people across state lines and promote international commerce. The circumstances of this case fit directly within the rule in *Moran v. Pyle*, and the same rule which supports the assertion and taking of jurisdiction by a foreign court must govern the recognition and enforcement of the judgment in this country.

The Uniform Law Conference of Canada has proposed legislation for the provinces setting out grounds for establishing a real and substantial connection. This draft legislation will be discussed elsewhere in this paper.

(c) **Forum Non Conveniens**

The *Morguard* case is significant in three aspects when dealing with actions involving the Internet: firstly, by requiring the application of the "real and substantial connection" test when deciding, in the first instance, whether a Canadian court should take jurisdiction over a foreign defendant (for example, if a foreign defendant causes damage to an Alberta resident by defaming that plaintiff on a website accessible to residents in Alberta);

---

79 See, for example, *Arrowmaster Incorporated v. Unique Forming Limited* 17 O.R. (3d) 407 (Gen. Div.); *Federal Deposit Insurance Corp. v. Vanstone* 88 D.L.R. (4th) 448 (B.C.S.C.); *Amopharm Inc. v. Harris Computer Corp.* (1992), 93 D.L.R. (4th) 524; *Clarke v. Lo Bianco* (1991), 84 D.L.R. (4th) 244; *TDI Hospitality Management Consultants Inc. v. Browne*; [1993] 3 W.W.R. 642; *Technaflow Inc. v. Minti Sales Ltd.* (1991), 81 Alta. L.R. (2d) 38.

80 *Moses v. North Shore Boat Builders* (1992), 68 B.C.L.R. (2d) 394 (S.C.); affirmed (1993), 83 B.C.L.R. (2d) 177 (C.A.) at 190.

secondly, in deciding whether to enforce the judgment of the court of a sister province; and thirdly, the "real and substantial connection" test must be applied by the Canadian courts when making a determination of whether or not to enforce the judgment of a foreign court in Canada.

Even if the connection between the defendant and the forum is sufficient to ground the court's jurisdiction to hear the matter, the court still has the discretion to deny the exercise of that jurisdiction.[81] To do so, the court applies the doctrine of *forum non conveniens* when a defendant applies to have the court exercise its jurisdiction to stay or dismiss the action on the basis that another forum is more closely connected to the events giving rise to the action or is otherwise a more appropriate forum for the adjudication of the parties' dispute.

This principle of *forum non conveniens* is a doctrine that should be applied in every case in which there exists an issue of conflicting jurisdictions. As stated by Justice Sopinka in *Amchem Products Inc. v. British Columbia (Workers' Compensation Board)*[82] the question to be asked is whether or not there is a more appropriate jurisdiction based on the relevant factors.[83]

> The choice of the appropriate forum is still to be made on the basis of factors designed to ensure, if possible, that the action is tried in the jurisdiction that has the closest connection with

---

81 The doctrine of *forum non conveniens* is equally applicable to those situation where the court's jurisdiction is based on the residence of the defendant.

82 *Amchem Products Inc. v. British Columbia (Workers' Compensation Board)* [1993] 3 W.W.R. 441.

83 *Amchem Products Inc. v. British Columbia (Workers' Compensation Board)* [1993] 3 W.W.R. 441 at 451.

> the action and the parties and not to secure a juridical advantage to one of the litigants at the expense of others in a jurisdiction that is otherwise inappropriate.

Justice Sopinka went on to say, however, that the existence of a more appropriate forum must be clearly established to displace the forum selected by the plaintiff. When applying the doctrine, each jurisdiction will apply its own principles to identify the most appropriate forum for the suit based on factors which connect the litigation and the parties' competing forums; essentially the same process used to apply the real and substantial connection test. It would appear, however, that the threshold test for determining jurisdiction, namely the real and substantial connection test, is much easier to meet than the test required to win in a competition between jurisdictions. When dealing with a question of jurisdiction, the court need only find *a* real and substantive connection, whereas in coming to a decision of which of two courts is the most appropriate, the court weighs these factors, and others, to determine which court has the *most* real and substantive connection with the action and the parties.[84]

D. Where are the Canadian Courts Headed?

(a) Assuming Jurisdiction When the Internet is a Connecting Factor

In the ensuing months, the courts in Canada will be faced with resolving the initial question of whether to take jurisdiction over an action where the key connecting

---

[84] See, for example, *Cunningham v. Hamilton* [1997] A.J. No. 1076. See also the discussion relating to the *Uniform Court Jurisdiction and Proceedings Transfer Act* discussed later in this paper.

factors between the defendant and the forum involve communication on the Internet. Is there any indication of how our courts will respond?

In the U.S., it appears that the courts look at both the nature of the claim together with the connection between the Internet activity and the cause of action to determine the issue. The courts in Canada will likely approach this question in a similar manner.

A review of the proposed *Uniform Jurisdiction Act* may give some indication of what would be sufficient to meet the real and substantial connection test when dealing with issues arising on an interprovincial level. The Uniform Law Conference of Canada has proposed a *Uniform Court Jurisdiction and Proceedings Transfer Act*[85] for adoption by all the provinces. The intention is to give statutory form to the substantive rules of jurisdiction as laid down by the Supreme Court of Canada, instead of leaving them implicit in the provincial rules for service of process. In fact, one purpose is to sever the connection between service and jurisdiction. Accordingly, the proposed Act should be a codification of the current law as interpreted by the drafters.

Jurisdiction of the court would be established by what the drafters call "territorial competence". A court would only have territorial competence in the following circumstances identified in the proposed section 3 to the Act:

> (a) that person is the plaintiff in another proceeding in the court to which the proceeding in question is a counterclaim,

---

[85] www.law.ualberta.ca/alri/ulc/acts/ejurisd.htm visited October 27, 1999.

(b) during the course of the proceeding that person submits to the court's jurisdiction,

(c) there is an agreement between the plaintiff and that person to the effect that the court has jurisdiction in the proceeding,

(d) that person is ordinarily resident in [*enacting province or territory*] at the time of the commencement of the proceeding, or

(e) there is a real and substantial connection between [*enacting province or territory*] and the facts on which the proceeding against that person is based.

Paragraphs (a), (b) and (c) reflect long standing law, whereas paragraphs (d) and (e) change the law by replacing the criteria for service of process with that of a substantive connection with the enacting jurisdiction.[86] As stated in the comments to section 3, paragraph (d) replaces "service" in the territory of the forum court with ordinary residence in that territory with the result that a person who is only temporarily in the jurisdiction will not automatically be subject to the court's jurisdiction. For a court to take jurisdiction over a person who is not ordinarily resident in its territory and does not consent to the court's jurisdiction, a real and substantial connection must exist within paragraph (e). Paragraph (e) would replace the various service ex juris rules in the provinces and bring the law and jurisdiction into line with the concept of "properly restrained jurisdiction" that the Supreme Court of Canada held was a pre-condition for the recognition and enforcement of a default judgment throughout Canada.

---

[86] *Canadian Conflict of Laws*, 4th ed. (Vancouver: Butterworths, 1997), J.G. Castel at 266.

Section 10 sets out a rebuttable presumption of what would constitute a real and substantial connection between a province and the facts on which a proceeding is based. The presumption set out in section 10 is based on the grounds for service ex juris found in the Rules of civil procedure of most provinces and includes those circumstances when an action:[87]

> (e) concerns contractual obligations, and
>
> (i) the contractual obligations, to a substantial extent, were to be performed in [*enacting province or territory*],
>
> (ii) by its express terms, the contract is governed by the law of [*enacting province or territory*],
>
> (iii) the contract
>
> (A) is for the purchase of property, services or both, for use other than in the course of the purchaser's trade or profession, and
>
> (B) resulted from a solicitation of business in [*enacting province or territory*] by or on behalf of the seller, ...
>
> (g) concerns a tort committed in [*enacting province or territory*],
>
> (h) concerns a business carried on in [*enacting province or territory*].

For contractual obligations, other than consumer transactions, the drafters are suggesting that a real and substantial connection requires that the contract was to be substantially performed

---

[87] Proposed Section 10.

in the province or that the contract is stated to be governed by that province's laws. For tort actions, if the tort was committed in the province, a real and substantial connection with that province is presumed.

The cases in the U.S. that are reviewed in this paper were actions based on either contract or tort. Dealing first with the contract actions, it is clear that if the parties have agreed to submit to the jurisdiction of the forum court, the defendant otherwise submits to the court's jurisdiction during the course of the proceedings, or the defendant is carrying on business or is ordinarily resident within the jurisdiction, the court will assume jurisdiction.[88]

Castel[89] suggests that if the contract is made in the jurisdiction, that would be sufficient to give the court jurisdiction under the Rules of many of the provinces, however, it is unlikely that this factor alone would be a sufficient connection to meet the test in *Morguard*.[90]

In the recent case of *Old North State Brewing Co. v. Newlands Service Inc.*[91] the B.C. Court of Appeal, in determining whether to enforce a default judgment granted by a court in North Carolina, based on an action for breach of contract, looked at all the

---

88 *Canadian Conflict of Laws*, 4th ed. (Vancouver: Butterworths, 1997), J.G. Castel at 206-208.

89 *Canadian Conflict of Laws*, 4th ed. (Vancouver: Butterworths, 1997), J.G. Castel at 208.

90 An earlier version of the Uniform Court Jurisdiction and Proceedings Transfer Act found in *Canadian Conflict of Laws*, 4th ed. (Vancouver: Butterworths, 1997), J.G. Castel at 228 included a provision which made the place where the contract was formed a basis for assuming jurisdiction. This was excluded in the most recent version of the proposed Act. It was pointed out in the commentary to the proposed section 10 that it is still open to the plaintiff to argue that the place of contracting is such a significant factor that the forum in which the contract is formed should exercise jurisdiction.

91 *Old North State Brewing Co. v. Newlands Service Inc.* [1998] B.C.J. No. 2472 (C.A.).

connecting factors between the defendant and North Carolina including Internet advertisements placed on the defendant's website. The court held that North Carolina had a real and substantial connection with the action based on the following factors:[92]

> The defendant portrayed itself as a corporate citizen that operated internationally rather than out of British Columbia by virtue of its Internet advertisements, the testimonial and photograph from Brooklyn, and its office in Sumas, Washington. In responding to enquiries from the plaintiff, the defendant sent promotional material to the plaintiff in North Carolina. The purchase order was executed by the plaintiff in North Carolina. The goods were delivered to the plaintiff in North Carolina. The defendant sent its representatives to North Carolina during the installation commissioning and repair of the brewing equipment it had supplied. The losses suffered by the plaintiff as a result of the installation of defective equipment were incurred in North Carolina.

There is no indication of the weight given by the court to the Internet advertisements, however the facts appear to lead to the conclusion that the contractual obligations were to be performed in North Carolina and therefore the defendant should reasonably expect to be haled into court in that jurisdiction. The circumstances in this case are analogous to those cases in the U.S. where the court found there was a business relationship between the parties and therefore had little hesitation in finding a real and substantial connection between the defendant and the jurisdiction.

In actions based on a breach of contract, the Internet will typically be only one of many factors that the court will have available to connect the defendant with the jurisdiction and it should be expected that the existence or non-existence of the Internet

---

92 *Old North State Brewing Co. v. Newlands Service Inc.* [1998] B.C.J. No. 2472 (C.A.) at Q.L., para 31.

connection will have little impact unless the court finds it necessary to determine where the contract was formed for reasons of validity.

The more interesting (and controversial) questions arise on the application of the principles in *Morguard* to tort actions where the Internet is a major factor. It is generally accepted that a province presumptively has jurisdiction if the proceeding is founded on a tort committed in that jurisdiction.[93] However, as Castel points out,[94] it is often a difficult task to determine the place of the tort.

In defamation actions, the place of the tort could be where the alleged defamatory statement was published, where the defamatory statement was originally uttered or where the victim suffered injury to his reputation. Publication takes place where the defamatory statements are heard or otherwise communicated,[95] whether or not the defendant intended that the statements be broadcast in the jurisdiction and arguably whether or not the plaintiff suffered damage in that jurisdiction.[96] In *Jenner v. Sun Oil Co.*,[97] the court stated that the publication of the defamatory statement is the very essence of defamation. The court reasoned at 537:

> A person may utter all the defamatory words he wishes without incurring civil liability unless they are heard and understood by a third person. I think it is a "startling

---

93 *Canadian Conflict of Laws*, 4th ed. (Vancouver: Butterworths, 1997), J.G. Castel at 209.

94 *Canadian Conflict of Laws*, 4th ed. (Vancouver: Butterworths, 1997), J.G. Castel at 209.

95 *Jenner v. Sun Oil Co.* [1952] 2 D.L.R. 526 (Ont. H.C.J.).

96 *Pindling v. National Broadcasting Corp.* (1984) 49 O.R. (2d) 58.

97 *Jenner v. Sun Oil Co.* [1952] 2 D.L.R. 526 (Ont. H.C.J.).

> proposition" to say that one may, while standing south of the border or cruising in an airplane south of the border, through the medium of modern sound amplification, utter defamatory matter which is heard in a Province in Canada north of the border, and not be said to have published a slander in the Province in which it is heard and understood. I cannot see what difference it makes whether the person is made to understand by means of the written word, sound-waves or ether-waves in so far as the matter of proof of publication is concerned. The tort consists in making a third person understand actionable defamatory material.

In *Jenner*, the plaintiff was an Ontario resident claiming that damage was caused to his reputation in Ontario from defamatory statements broadcast by the U.S. defendants on a radio network located in New York which were heard in Ontario. The court concluded that the fact the statements were made in New York did not matter if "they were so transmitted as to be published within the jurisdiction in such a manner as to be likely to cause the plaintiff to suffer substantially in his reputation in Ontario".[98] In *Pindling v. National Broadcasting Corp.*, the defendant was denied a motion to set aside service ex juris on similar facts, except that in this case the plaintiff had no connection to the forum and the signals broadcast by the defendant were retransmitted by others from the U.S. into Ontario, and the defendant had no control over such transmission by third parties.

In *Direct Energy Marketing Ltd. v. Hillson* [1999] A.J. No. 695, the residence of the plaintiff in the forum was held to be the determining connecting factor in a defamation action.[99]

---

98 *Jenner v. Sun Oil Co.* [1952] 2 D.L.R. 526 (Ont. H.C.J.) at 537.

99 In this case, the plaintiff alleged that the defamatory statements were published in two newspapers in Saskatchewan, several copies of which were sold in Alberta, and also alleged that the defamatory statements were published on the Internet sites of those newspaper and were therefore "published"

If the reasoning in the above cases is applied, our courts may take jurisdiction over foreign defendants based solely on the fact that defamatory statements made by the defendant were available and read by someone within the forum, whether or not the statements caused damage to the plaintiff in that jurisdiction. Whether the defendant intended that the statements be read by persons in the forum is irrelevant. In the U.S.,[100] in contrast, a passive website containing defamatory statements would not be enough to meet the "minimum contacts" test in circumstances where the defendant does not target or solicit residents of the forum, unless the defendant "does something more" within the forum.[101]

Negligence actions are slightly different, in that three elements are necessary to establish a cause of action: a duty of care owed to the plaintiff, a breach of that duty and resultant damage. All three elements may occur in different jurisdictions and the courts have to choose which element constitutes the "place of the tort". If an action is against a foreign defendant, or against a defendant in a sister province based on the tort of negligence, the jurisdictional question may again be resolved by looking to where the tort is committed. In *Moran v. Pyle National (Canada) Ltd.*[102] the Supreme Court of Canada held that it is unnecessary and unwise to resort to any arbitrary set of rules, as the place of acting or the

---

in Alberta. The court did not have to address the issue of whether the Internet access was a sufficient connecting factor as the parties did not contest the Master's findings that the court had jurisdiction. The only issue was whether the *forum non conveniens* test was properly applied. For a contrary opinion with respect to the residence of the plaintiff being a sufficient connecting factor, see *Webb v. Hooper* [1994] A.J. No. 335.

100 *Barrett v. The Catacombs Press*, No. 99-736 (D.C.E.D. Pa. April 12, 1999).

101 *Blumenthal v. Drudge*, 992 F.Supp. 44 (D.D.C. 1998).

102 [1975] 1 S.C.R. 393.

place of injury theories are too arbitrary and too inflexible to achieve a just result in all cases. However, for jurisdictional purposes, the court stated that a real and substantial connection exists, and a court is entitled to exercise jurisdiction over a foreign defendant, if the damage to the plaintiff was caused in the forum jurisdiction and such damage was reasonably foreseeable. Arguably, where the tort is committed and where the damage occurs should only be some of the factors that are considered in coming to the decision of whether a real and substantial connection exists.

Should the principles in *Moran* be extended to medical malpractice cases where a person suffers damage arising from the incorrect advice given by a doctor over the Internet? Would the residence of the plaintiff be enough of a connection for the court to take jurisdiction, based on the argument that the pain and suffering, and therefore the damage, was caused in that forum? If the defendant ought reasonably to have foreseen that persons in other jurisdictions would be relying on that advice, that should be enough to establish the connection. With the growth of what is called "cybermedicine",[103] the courts will have to grapple with the issue of who has jurisdiction over medical malpractice occurring over the Internet.

It is currently a matter of speculation whether a Canadian court would take jurisdiction over a foreign defendant based on the claim that the defendant was infringing the plaintiff's trademark by using a similar name on a website to which residents of the forum had access. If damage is caused to the plaintiff in the forum, in light of the *Moran* decision,

---

[103] Barbara Tyler "Cyberdoctors: The Virtual Housecall - The actual practice of medicine on the Internet is here; is it a telemedical accident waiting to happen?" 31 Ind. L. Rev. 259 (1998).

that may be all that is necessary to show a real and substantial connection with the jurisdiction. If so, the Canadian courts may take jurisdiction even in those circumstances where the defendant is merely operating a passive website, a broader ground then that currently required to meet the "minimum contacts" required in the U.S.[104]

Even if it appears that the forum court has the constitutional ability to accept jurisdiction, it must be remembered that it is still open to that court to deny the exercise of its jurisdiction on the basis of *forum non conveniens*, if raised and argued by the defendant. Where a defendant does not defend the action brought in Canada, however, the question of whether or not the forum has the *most* real and substantial connection with the defendant or the action is usually not addressed. In such circumstances, the plaintiff only needs to satisfy the minimal jurisdictional requirements of the existence of *a* real and substantial connection with the defendant or the action. As indicated previously, the connection with the forum can be 'anything' and a passive website accessible in the forum, similar to that described in *Inset Systems Inc., supra*, may be a sufficient connection to ground jurisdiction in tort actions brought in Canada.

(b) **Enforcement of Foreign Judgements**

In *Morguard*, the court was dealing with comity between provinces and the enforcement of judgments of other Canadian courts, not enforcement of foreign judgments.

---

104 See, for example the cases of *Patriot Systems v. C-cubed Corporation* and *Weber v. Jolly Hotels, supra*.

However, Canadian courts have typically used the same test for enforcement of both interprovincial judgments and those granted by foreign courts.[105]

This problem was compounded by the Supreme Court in *Amchem Products Inc. v. British Columbia (Workers' Compensation Board)*.[106] In *Morguard* it was unnecessary for the court to consider the case of competing jurisdictions and the question of comity between competing nations. In *Amchem,* however, the court was required to address this issue directly. At issue in *Amchem* was the determination of which principles are to be applied when a court exercises its discretion to grant an anti-suit injunction. An anti-suit injunction is a remedy which may be granted by a domestic court upon the request of a defendant to prevent a plaintiff from continuing a foreign action against that defendant. A similar remedy (a stay) would be available to a defendant in an action commenced in a domestic forum that the defendant feels is more appropriately decided in another forum.

As stated by Sopinka, J.:[107]

> Although the remedy of a stay and an injunction have as their main objectives the selection of an appropriate forum for the trial of the action, there is a fundamental difference between them which is crucial to the development of the principles which should govern each. In the case of the stay the domestic court determines for itself whether in the circumstances it should take jurisdiction whereas, in the case

---

105 See *Moses v. North Shore Boat Builders* 68 B.C.L.R. (2d) 394 (S.C.); affirmed (1993), 83 B.C.L.R. (2d) 177 (C.A.); *Old North State Brewing Co. v. Newland Services Inc.* [1998] B.C.J. No. 2474; see also references at note 76.

106 *Amchem Products Inc. v. British Columbia (Workers' Compensation Board)* [1993] W.W.R. 441.

107 *Amchem Products Inc. v. British Columbia (Workers' Compensation Board)* [1993] 3 W.W.R. 441 at Q.L., p. 32.

> of the injunction, it in effect determines the matter for the foreign court.

In the later case, the question of comity needs to be addressed, and therefore the Supreme Court has stipulated a two part test when deciding whether to grant an anti-suit injunction: first, the domestic forum is to apply the principles of *forum non conveniens* to determine whether the foreign court "could reasonably have concluded there was no alternative forum that was clearly more appropriate"[108] and, if so, it should deny the application. If the domestic court reasonably concludes that the foreign court assumed jurisdiction on a basis that was inconsistent with the principles of *forum non conveniens*, it must then go to step two of the analysis and determine if, as a result of the foreign court taking jurisdiction, a serious injustice will occur.

As stated by Sopinka, J.:[109]

> The result of the application of these principles is that when a foreign court assumes jurisdiction on a basis that generally conforms to our rules of private international law relating to the forum non conveniens, that decision will be respected and a Canadian court will not purport to make the decision for the foreign court. The policy of our courts with respect to comity demands no less. If, however, a foreign court assumes jurisdiction on a basis that is inconsistent with our rules of private international law and an injustice results to a litigant or "would be" litigant in our courts, then the assumption of jurisdiction is inequitable and the party invoking the foreign jurisdiction can be restrained. The foreign court, not having, itself, observed the rules of comity, cannot expect its decision to be respected on the basis of comity.

---

108 *Amchem Products Inc. v. British Columbia (Workers' Compensation Board)* [1993] 3 W.W.R. 441 at Q.L., p. 9.

109 *Amchem Products Inc. v. British Columbia (Workers' Compensation Board)* [1993] 3 W.W.R. 441 at Q.L., p. 11.

Should the Canadian courts have a discretionary right to refuse to recognize and enforce a foreign judgment on the grounds that the action should have been stayed or dismissed by the original court on the ground of *forum non conveniens*? If not, is it reasonable to apply the two part test set out in *Amchem* in the interest of comity?

The Supreme Court has made it clear that the foreign court need not apply the *forum non conveniens* test when making its decision, but rather "it is the result of the decision when measured against our principles that is important and not necessarily the reasoning that leads to the decision".[110]

If our courts determine that the more stringent test in *Amchem* is the appropriate test, caution should be exercised when applying the first part of the test. Even in *Amchem*, it is submitted, the court did not apply its own test correctly. Sopinka, J. reviewed the evidence and found that the Texas court had complied with the due process requirements of the Fourteenth Amendment to the Constitution of the United States, and that the "minimum contacts" test had been satisfied. Sopinka J. stated:[111]

> In my opinion, the application of this provision, which is a constitutional requirement, is consistent with our rules of private international law relating to forum non conveniens.

The application of these principles is not the same as our test for *forum non conveniens*. It is only consistent with our jurisdictional test of a real and substantial connection. As we have seen from the foregoing examples, the U.S. courts, when applying

---

110 *Amchem Products Inc. v. British Columbia (Workers' Compensation Board)* [1993] 3 W.W.R. 441 at Q.L., p. 76.

111 *Amchem Products Inc. v. British Columbia (Workers' Compensation Board)* [1993] 3 W.W.R. 441 at Q.L., p. 77.

the "minimum contacts" test are not asking whether the forum court has the *most* contacts with the action or the defendant, but merely whether it has met the minimum jurisdictional requirement as set out in *International Shoe Co. v. Washington.*[112] No comparative analysis takes place at this stage of inquiry, if at all.

The concern, of course, is that the lower courts will apply *Morguard* and *Amchem* in coming to a decision to enforce a foreign judgment against a Canadian defendant that had minimum contacts with the foreign jurisdiction, similar to the circumstances in *Inset Systems, Inc.*[113] If so, Canadians doing business through the Internet need to know that even minimum contacts with a state sufficient to meet that state's constitutional requirements will be enough for our courts to enforce any resulting judgment against their assets in Canada, whether or not the contacts with that state would have been sufficient for our court to decline jurisdiction in similar circumstances based on application of the *forum non conveniens* test.

Canada's first major judgment applying the "real and substantive connection" test in addressing whether to enforce a foreign judgment where one of the key connecting factors was the Internet was delivered by the B.C. Court of Appeal in March of 1999. Leave to appeal was denied by the Supreme Court of Canada. In *Braintech, Inc. v. Kostiuk,*[114] the plaintiff, Braintech, was a software development company incorporated in Nevada with corporate offices located in Vancouver and research and development facilities in Austin,

---

112 *International Shoe Co. v. Wash*, 326 U.S. 310 (1945).

113 *Inset Systems, Inc. v. Instruction Set, Inc.*, 937 F.Supp. 161 (D.Comm.1996).

114 *Braintech, Inc. v. Kostiuk* [1999] B.C.J. No. 622 (BCCA), appeal to S.C.C. denied [1999] S.C.C.A. No. 236.

Texas. Kostiuk was alleged to have used the Internet to transmit and publish defamatory information about Braintech through a bulletin board known as the "Silicon Investor". The Silicon Investor was available for interested persons to discuss and exchange information regarding technology stocks and investments and was readily available to residents of Texas. Braintech, a publicly traded company, commenced an action in Texas against Kostiuk claiming damages for the electronic transmission and publication of defamatory statements posted on the Silicon Investor. Kostiuk did not defend the action and the court held in favour of Braintech, granting damages in the amount of U.S.$300,000. As Kostiuk was a resident of British Columbia, and presumably had assets there, Braintech commenced an action in British Columbia in order to enforce its judgment in that province. In April of 1998, Braintech obtained a judgment in its favour which was appealed by Kostiuk.

The question before the Court of Appeal was whether there was a real and substantial connection between Texas and either the defendant, or the wrongdoing alleged to have taken place in that state. If there was such a connection, the B.C. court would uphold the lower court's decision to enforce the judgment obtained by the plaintiff in Texas. If such a connection did not exist, however, the judgment would not be enforced.

The Texas court had based its jurisdiction on the state's long arm statute which provided that a non-resident does business within Texas if it commits a tort in whole or in part within the state. If the court found that Kostiuk's action constituted a tort committed in Texas, it was entitled under its laws, subject to the "due process" requirement, to assume jurisdiction over the cause of action.

In reasons delivered April 2, 1998 by the B.C. Supreme Court Chambers Judge, it was held:[115]

> The Plaintiff, at the time of the alleged torts, maintained an office in Austin, Texas carrying out research and development, marketing and investor relation activities. The plaintiff's chief technology officer and director resided and worked in Austin, Texas. The damages in part were incurred in Texas by means of Internet publications. The defendant's defamation was found to have been published in Texas.

If, in fact, the tort of defamation occurs where the publication occurs,[116] then, according to the reasoning of the trial judge, it occurs everywhere there is access to the defamatory material, and therefore, arguably it occurs everywhere. It is not unlike those cases where a defamatory statement is "published" on a national broadcast. As discussed in *Digital Equipment Corp. v. Altavista Tech., Inc.*,[117] and *Barrett v. The Catacombs Press*,[118] such publication is insufficient to ground general jurisdiction over a defendant in the U.S., but it may be sufficient to allow the court to assume specific jurisdiction if such action is the very act complained of by the plaintiff and there are other factors, such as a business relationship or contract, connecting the plaintiff resident in the forum state with the non-resident defendant.

No such other factors existed in this case, and the B.C. Court of Appeal was not prepared to find that the "transitory, passive presence in cyberspace of the alleged

---

115 *Braintech, Inc. v. Kostiuk* [1998] B.C.J. No. 3201 (BCSC), appeal to S.C.C. denied [1999] S.C.C.A. No. 236 at Q.L., para 20.

116 *Jenner v. Sun Oil Company Ltd.* [1952] O.R. 240 (Ont.H.C.).

117 *Digital Equip. Corp. v. Altavista Tech., Inc.*, 960 F.Supp. 456 (D.Mass.1997).

118 *Barrett v. The Catacombs Press*, No. 99-736 (D.C.E.D. Pa. April 12, 1999).

defamatory material"[119] constituted a sufficient connection between Texas and the defendant or the subject matter of the case.

Goldie J.A., applying the principles set out in *Amchem*, first considered whether the Texas court, when claiming jurisdiction, had departed "from our own test of *forum non conveniens* to such an extent as to justify our courts in refusing to respect the assumption of jurisdiction by the foreign court [and if, in the] circumstances such assumption amounts to a serious injustice".[120] Was the alleged publication of a libel which affected the interests of present and potential investors resident in Texas sufficient for the Texas court to take jurisdiction, as claimed by the Plaintiffs? "Only if the mode of communication through the Internet supports this conclusion".[121] Goldie, J.A. went on to state that "libel is only committed when the defamatory material is published to at least one person other than the complainant".[122] The court went on to find that the bulletin board Silicon Investor was a passive site:[123]

> ... accessible only to users who have the means of gaining access and who exercise that means. In these circumstances the complainant must offer better proof that the defendant has entered Texas than the mere possibility that someone in that

---

119 *Braintech, Inc. v. Kostiuk* [1999] B.C.J. No. 622 (BCCA), appeal to S.C.C. denied [1999] S.C.C.A. No. 236 at Q.L., para 65.

120 Quoting *Amchem Products Inc. v. British Columbia (Workers' Compensation Board)* [1993] 1 S.C.R. 897 at 914.

121 *Braintech, Inc. v. Kostiuk* [1999] B.C.J. No. 622 (BCCA), appeal to S.C.C. denied [1999] S.C.C.A. No. 236 at Q.L., para 58.

122 *Braintech, Inc. v. Kostiuk* [1999] B.C.J. No. 622 (BCCA), appeal to S.C.C. denied [1999] S.C.C.A. No. 236 at Q.L., para 59.

123 *Braintech, Inc. v. Kostiuk* [1999] B.C.J. No. 622 (BCCA), appeal to S.C.C. denied [1999] S.C.C.A. No. 236 at Q.L., para 62 and 65.

> jurisdiction might have reached out to cyberspace to bring the defamatory material to a screen in Texas.
>
> No further proof was provided:[124]
>
> In the circumstances of no purposeful commercial activity alleged on the part of Kostiuk and the equally material absence of any person in that jurisdiction having "read" the alleged libel all that has been deemed to have been demonstrated was Kostiuk's passive use of an out of state electronic bulletin. The allegation of publication fails as it rests on the mere transitory, passive presence in cyberspace of the alleged defamatory material; such a contact does not constitute a real and substantial presence. On the American authorities this is an insufficient basis for the exercise of an in personam jurisdiction over a non-resident.

Clearly, in the court's view, Texas had departed from their own test of "minimum contacts" and should not have exercised jurisdiction.

Goldie, J.A. set out additional reasons why Texas was "not even an appropriate forum"[125] including: Kostiuk's only connection with Texas was "deemed" by virtue of the allegation that he committed a tort in Texas; Braintech was incorporated in Nevada and domiciled in B.C. and had no presence in Texas since December 1996. Most importantly, to enforce recovery of the default judgment obtained in Texas on the deemed proof of use of an electronic bulletin board would encourage a multiplicity of actions the world over wherever the Internet was available.[126]

---

124 *Braintech, Inc. v. Kostiuk* [1999] B.C.J. No. 622 (BCCA), appeal to S.C.C. denied [1999] S.C.C.A. No. 236 at Q.L., para 65.

125 *Braintech, Inc. v. Kostiuk* [1999] B.C.J. No. 622 (BCCA), appeal to S.C.C. denied [1999] S.C.C.A. No. 236 at Q.L., para 66.

126 *Braintech, Inc. v. Kostiuk* [1999] B.C.J. No. 622 (BCCA), appeal to S.C.C. denied [1999] S.C.C.A. No. 236 Q.L., para 66.

In *Amchem*, the Supreme Court stated that our courts must first ask whether the result of the decision made by the foreign court is consistent with the result that would have been found if the foreign court had applied our principles of *forum non conveniens*. The Supreme Court further reasoned that if the foreign U.S. court reasonably found that the defendant had the necessary "minimum contacts" with the state, and met the due process requirement of the Fourteenth Amendment to the U.S. Constitution, then that would be sufficient to satisfy our test of *forum non conveniens*. Even if the first prong of the test is not satisfied, and it is found that the foreign court should not have taken jurisdiction when tested against our principles of *forum non conveniens*, *Amchem* requires the court to go on to ask whether an injustice would result. In circumstances where the question before the court is the recognition of a foreign judgment, rather than an anti-suit injunction, it would appear that the second prong would require a determination of whether the recognition of the foreign court's judgment would result in an injustice to the defendant.

In *Braintech*, the court, by finding that there were insufficient connections between the Texas court and either the defendant or the action, did not have to deal with the thornier question of whether or not meeting the minimum contacts test for jurisdiction in the U.S. was equivalent to the principles of *forum non conveniens*. Goldie, J.A. stated the issue before the court as being whether there was a "real and substantial connection between Texas and the wrongdoing alleged to have taken place in that state" [127] yet Goldie only hints at this

---

127 *Braintech, Inc. v. Kostiuk* [1999] B.C.J. No. 66 (BCCA), appeal to S.C.C. denied [1999] S.C.C.A. No. 236 at Q.L., para 2.

issue by stating:[128] "[if] the obligation to defer to the comity which is to be accorded the default judgment of the [foreign court] is to be tested by the principle of *forum non conveniens* some flesh must be put on the bare bones of "real and substantial connection"." Possibly what Goldie is referring to in this comment is the concern raised earlier that the test for a real and substantial connection, when dealing with interprovincial judgments, is a low threshold of jurisdictional competence which requires "more flesh on the bones" when being applied to the recognition of a judgment of a foreign court. Late in the judgment Goldie refers to the transitory presence of the defendant as not constituting a "real and substantial presence".[129] However, the court seems to be applying the test as discussed in *Zippo Mfg.*[130] rather than the Canadian test as set out in *Morguard*.

Breaches of contractual obligations are relatively easy to deal with and the courts in the U.S. have, with some exceptions, come to decisions that accord with our sense of "fair play" when determining jurisdiction. The same is true when there is active solicitation by the defendant in the plaintiff's chosen forum, and in cases where infringement of the plaintiff's trademark is claimed. It is defamation cases like *Braintech* and negligence cases which will arise from activities like "cybermedicine" that will be very difficult to deal with when faced with jurisdictional and enforcement issues.

On the one hand, there is concern that "robust debate" and "fair comment" will be curtailed if the courts expose participants to litigation everywhere. On the other

---

128 *Braintech, Inc. v. Kostiuk* [1999] B.C.J. No. 622 (BCCA), appeal to S.C.C. denied [1999] S.C.C.A. No. 236 at Q.L., para 56.

129 *Braintech, Inc. v. Kostiuk* [1999] B.C.J. No. 622 (BCCA), appeal to S.C.C. denied [1999] S.C.C.A. No. 236 at Q.L., para 65.

130 *Zippo Mfg. Co. v. Zippo Dot Com, Inc.*, 952 F. Supp 1119 (W.D.Pa.1997) at 1125.

hand, an individual has intentionally caused damage to another and the state has an interest in protecting its citizens. Clearly, something more than the actual viewing of alleged defamatory material by a person in the forum state should be required in order for a court to assume jurisdiction; and the fact that the forum state is the plaintiff's domicile (and therefore worthy of protection by the state) should not be sufficient to meet the "purposeful availment" prong of the minimum contacts test nor should it be sufficient to meet the *Amchem* test for enforcement of a foreign judgment. However, those factors, in conjunction with others, may be enough to put an individual on notice that he or she may be haled into court in that jurisdiction.

3. INTERACTION WITH CUSTOMERS

A. Sale of Products

(a) Commercial Transactions Generally

Interprovincial sales in Canada raise few conflict issues, as the law pertaining to the sale of goods is the same, with a few minor exceptions, in all the common law provinces and the territories.[131] Quebec has its own regime which, unlike the other provinces, is not based on the common law imported into Canada at the time of Confederation.

A sale of goods or services between parties in different jurisdictions, both on and off the Internet, gives rise to the issues of determining what law governs the formalities of the contract, its validity, the obligations of the parties and when and how property in the goods is transferred. The Internet, however, adds one new element in the transaction that

---

131 *Sale of Goods in Canada*, 4th ed. (Scarborough: Carswell, 1995), G.H.L. Fridman at 471.

introduces an element of uncertainty in a number of areas, including the applicability of international conventions, when and where a contract created on the Internet is formed, and a host of other issues that must be considered by the e-businessman in determining his obligations and his risks of conducting business on the Internet.

(b) **When is a Contract Formed on the Internet?**

One of the primary matters to be addressed by a person wishing to conduct business on the Internet is to ensure that a valid and enforceable contract is formed between the vendor and the purchaser of the goods or services. In some instances, the entire contract can be made and performed on the Internet as, for example, when the vendor licenses software to a purchaser which is then downloaded onto the purchaser's computer. In other transactions, the contract is made on the Internet, but external action is required, such as the delivery of the product to the purchaser, which can either be a tangible good or the provision of a service.

The legal requirements for a contract made through the Internet are the same as if they were made orally or in writing. In addition to other requirements, such as consideration, there must be an offer which has been communicated by the offeror and the offeree must have accepted and in some manner communicated to the offeror within the time available for acceptance. In the U.S., an offer may be accepted "in any manner and by any medium reasonable in the circumstances."[132] Accordingly, an offer made by e-mail should be capable of being accepted by e-mail unless the offeror stipulated a different mode of acceptance in the e-mail that contained the offer.

---

132 UCC, s. 2-206(1)(a).

When considering jurisdictional questions, where the contract is formed may be a significant factor in determining 'minimum contacts' or 'a real and substantial connection' with the forum. One must determine when and where a contract is formed by an exchange on the Internet. Generally, under Canadian law, a contract is formed in the place where and when the acceptance is received. One exception to this general rule is the 'postal rule' which states that a contract is formed where and when an acceptance is put in the mail, whether or not it is ever received by the other party.[133]

In the very recent case of *Eastern Power Ltd. v. Azienda Communale Energia and Ambiente*[134] the Ontario Court of Appeal considered this issue in the context of an acceptance communicated by facsimile transmission. In this case, the plaintiff signed a letter of intent in Ontario and faxed it back to the defendant Azienda, in Rome. The plaintiff argued that facsimile transmissions should follow the postal rule exception, and therefore the contract would be formed in Ontario. The court disagreed, holding instead that when an offer is accepted by facsimile the contract is formed in the place where the acceptance is received. The court preferred the analysis of the House of Lords in *Brinkibon Ltd. v. Stahag Stahl G.m.b.H.*, [1983] 2 A.C. 34 (H.L) where Lord Brandon, analyzing the applicability of the postal rule to an acceptance by telex, stated, at p. 48:

> The general principle of law applicable to the formation of a contract by offer and acceptance is that the acceptance of the offer by the offeree must be notified to the offeror before a contract can be regarded as concluded. The cases on acceptance by letter and telegram constitute an exception to

---

133 Fridman, *The Law of Contract in Canada*, 3rd ed., (Carswell: Toronto, 1994) at 65 – 68.

134 *Eastern Power Ltd. v. Azienda Communale Energia and Ambiente*, [1999] O.J. No. 3275, Docket No. C31224 (Ont. C.A.).

> the general principle of the law of contract stated above. The reason for the exception is commercial expediency. That reason of commercial expediency applies to cases where there is bound to be a substantial interval between the time when the acceptance is sent and the time when it is received. In such cases the exception to the general rule is more convenient, and makes on the whole for greater fairness, than the general rule would do. In my opinion, however, the reason of commercial expediency does not have any application when the means of communication employed between the offeror and the offeree is instantaneous in nature, as in the case when either the telephone or telex is used. In such cases the general principle relating to the formation of contracts remains applicable, with the result that the contract is made where and when the telex of acceptance is received by the offeror (case citations omitted).

The Court of Appeal held that communications by facsimile are the "simple case of instantaneous communication between principles" and therefore the general rule of contract formation is to be applied. There is no reason to suggest that communication by e-mail should be treated any differently.

Persons doing business on the Internet in Canada would be well advised to ensure that contracts created through communications on the Internet are formed (accepted) in their home jurisdiction as this will be a significant factor in the court's determination of whether minimum contacts exist, or in Canada whether or not there is a real and substantial connection between the defendant, the action and the forum. It is also a significant factor in deciding which jurisdiction has the 'closest connection' with the parties and the action when applying the test of *forum non conveniens*.

(c) **Contract Terms**

Contracts for the sale of goods, including Internet transactions, are generally governed by sale of goods legislation in each province in Canada and by the *Uniform*

Commercial Code in the U.S. How does the e-businessman know, however, which legislation to comply with, or must he comply with the legislation in every jurisdiction in which his products are sold?

If the matter is before a Canadian court, either to impose a province's sale of goods legislation on the defendant, or in circumstances where the plaintiff is trying to enforce a foreign judgment in Canada, the court will look at the factors that create a real and substantial connection between the parties and the jurisdiction. One of those factors will be the place the contract is formed. If the e-businessman had ensured that contracts are accepted in his home jurisdiction, the Ontario decision in *Eastern Power* [135] would suggest that the contract is formed where the e-businessman accepted the contract.[136] It is unlikely that this factor alone would be determinative for the purposes of jurisdiction under either the existing rules of court or the proposed *Uniform Court Jurisdiction and Proceedings transfer Act*, nor would it be a sufficient connection to meet the test in *Morguard Investments Ltd. v. De Savoye*[137] It would, however, be persuasive both for the purposes of determining jurisdiction and for the conflict of law question of whose law applies.

The choice of forum and choice of law stipulated by the e-businessman and included in his 'click wrap' agreement or contract created on-line is more likely to be upheld

---

135 *Eastern Power Ltd. v. Azienda Communale Energia and Ambiente,* [1999] O.J. No. 3275, Docket No. C31224 (Ont. C.A.).

136 There is still an issue, however, of whether the contract is accepted when and where the contract is received by the server or by the individual operating the web page. The decision of the *Copyright Board, Supra,* would suggest that where the server is located is the key factor. The proposed *Uniform Electronic Commerce Act* would deem the electronic document to be received at the addressee's place of business, and,, if the addressee has more than one place of business, at that place which has the closest relationship to the underlying transaction.

137 *Morguard Investments Ltd. v. De Savoye* [1990] 3 S.C.R. 1077.

by the courts following the decision in *Rudder v. Microsoft Corp.*[138] This permits the e-businessman to gain some measure of control over which courts may assume jurisdiction as well as the contractual terms that will be imposed on his transaction by legislation.

(d) ***Uniform Electronic Commerce Act***

Numerous bodies have been working on proposals to bring some sense of certainty to the area of e-commerce. One such body is the United Nations Commission on International Trade Law (UNCITRAL) which, since 1985 has had a significant involvement in computer related matters.[139] In the mid-1990's, it took particular notice of the increasing number of transactions in international trade that were carried out by means of electronic data interchange and other means of e-commerce involving the use of alternatives to paper-based forms of communication and storage of information. UNCITRAL has sought to fulfill its mandate, which is to further the progressive harmonization and unification of the law of international trade, by expanding its involvement from EDI and EFT transactions to e-commerce standards. In so doing UNCITRAL, on June 12, 1996, adopted a model law that would facilitate "...the use of electronic commerce, [which would be] acceptable to States

---

138 *Rudder v. Microsoft Corp.*, Ontario Superior Court of Justice, October 8, 1999.

139 http://www.uncitral.org/en-index.htm The United Nations Commission on International Trade Law (UNCITRAL) was established by the United Nations General Assembly in 1966. The Commission is regarded as the core legal body of the United Nations system in the field of international trade law and the main vehicle by which the United Nations can play a more active role in reducing and removing obstacles to the flow of trade. The general mandate of the Commission is to further the progressive harmonization and unification of international trade law and to remove unnecessary obstacles to international trade caused by inadequacies and divergence in national legislation affecting trade. The Commission has carried out work in eight different areas of trade law including: international sale of goods and related transactions; international transport of goods; international payments (Legal Guide on Electronic Fund Transfers, Model Law on International Credit Transfers); international commercial arbitration and Electronic Commerce (Model Law). To develop the preparatory work on topics within the Commission's program areas, UNCITRAL established three Working Groups currently named the Working Group on International Contract Practices, the Working Group on Insolvency Law and the Working Group on Electronic Commerce.

with different legal, social and economic systems, [while contributing] to the development of harmonious international economic relations." (the *UNCITRAL Model Law on Electronic Commerce* or "Model Law"[140]).

Recognizing the dramatic and explosive growth of the Internet and e-commerce, as well as the deficiencies in modern day legislation, the United Nations resolved to adopt the UNCITRAL Model Law on Electronic Commerce as a guide for states to harmonize and unify international trade laws. In response, the Uniform Law Commission has adopted the Uniform Electronic Commerce Act ("UECA") as model "enabling" legislation to provide certainty among private parties while establishing a framework for e-communication with government. The new legal frameworks proposed by the Model Law remove barriers for e-commerce by making the law "media neutral" and flexible to accommodate the radical changes so prevalent in information technology. The new legislation also provides much needed clarification on contractual issues arising from communicating electronically, and establishes greater certainty with respect to the formation of on-line contracts, including electronic signatures.

In Canada, the challenges posed by an increasingly global and digitally-driven economy are being addressed at different levels. At the federal level, there are currently two major initiatives: Bill C-6 (formerly Bill C-54), the *Personal Information Protection and Electronic Documents Act*; and the Government of Canada's Public Key Infrastructure (PKI) Initiative. These initiatives are the means by which the federal Department of Justice seeks to establish a legal framework to provide Canadians security and confidence in the utilization

---

140 UNCITRAL Model Law on Electronic Commerce with Guide to Enactment (1996), with additional article 5 as adopted in 1998.

of the Internet as a place to communicate and to conduct business, and to facilitate e-commerce[141] nationally and internationally in a secure environment.

Parliament has adopted the principles of the Model Law in Part II of Bill C-6. In Part II of the *Personal Information Protection and Electronic Documents Act* a legislative scheme is set out whereby requirements in federal statutes and regulations that contemplate the use of paper or do not expressly permit the use of electronic technology may be administered or complied with using electronic means.

In essence, Bill C-6 authorizes ministers of the federal government to establish rules on how individuals may satisfy, by electronic means, the legal requirements for writing, signatures, originals and the filing of specified forms in their dealings with the federal government. The legislation does not apply to relationships between private parties as this falls within provincial jurisdiction.

While recognizing the provinces' constitutional jurisdiction over property and civil rights, the federal Department of Justice has nonetheless played a key role in the Uniform Law Conference of Canada (ULCC)[142] in drafting the proposed provincial

---

141 The federal government defines e-commerce as: broadly, including any transaction where the underlying means of facilitating that transaction is electronic, and which is also used to deliver government services.

142 The ULCC's mandate is to harmonize the Canadian statute law where harmony is beneficial. It does so by preparing uniform statutes that it recommends for enactment by the provinces and territories and sometimes by the federal government as well. It also does so by adopting uniform statutes dealing with the choice of law. On occasion it promotes particular provisions for statutes or publishes guides to uniform legal procedure.

legislation, namely the *Uniform Electronic Commerce Act* (UECA).[143] In adopting the UECA in 1998, the ULCC sought to address two fundamental issues:[144]

1) How should the principles of the UN Model Law be implemented in Canada?

2) How can the UECA reduce the legal uncertainty surrounding statutory rules that require writing, or signatures, or the use of original documents?

The UECA's purpose is to create legal certainty in the area of "data messaging" where there currently exists legal uncertainty to promote the appropriate transition from a paper based economy, where statutory and legal rules require some documents to be "in writing", to be "signed by the parties", to be "witnessed" with special effect given to the "original" document, to an e-commerce economy, where intention can be communicated automatically, or by symbolic actions like clicking on an icon on a computer screen. The UECA's primary focus is to provide a framework to ensure the intentions of the parties, so critical for legal relationships, are adequately addressed. In fact, the UECA applies beyond the scope of "commerce", to almost any legal relationship that may require documentation.

The UECA's Fundamental Principles

As discussed in the commentary to the UECA, the UECA embodies three fundamental principles:

---

143 http://www.law.ualberta.ca/alri/ulc/current/euecafa.htm

144 The background comprising the UECA is addressed at: http://www.law.ualberta.ca/alri/ulc/eindex.htm

1. Conducting business or communicating by electronic means is optional, not mandatory.

Nothing in the UECA requires a person to use or accept information in electronic form.[145] The legislation is intended to be enabling, thereby giving parties the freedom to choose how they wish to transact business. Provision is made for exceptions, such as wills, powers of attorney, and similar documents, where it is expected that specific rules will have to be established to ensure safeguards for their users.

Communications with governments are dealt with separately, allowing the government to set its own rules (and timing) for accepting incoming electronic documents. Outgoing documents, however, will generally have to conform to the general standards of the UECA.

2. Electronic documents are given the same legal status or effect as their paper-based counterparts.

The UECA's legislative technique is to make electronic documents equivalent to paper documents.[146] These electronic documents are then superimposed onto the body of statutory and case law encompassing such requirements as "in writing", "signed" by the maker or to be the "original". This technique eliminates the need to amend the vast array of statutes that were passed before electronic communication was even contemplated.

3. Questions of capacity ("Am I allowed to do this electronically?") are transformed into questions of proof ("Have I met the standard?").

---

145 UECA, section 6(1).

146 UECA, Part I .

The UECA seeks to remove doubt about whether a document can be electronically 'signed' by providing that the maker of a document can create his own 'electronic signature' on an attached or associated document that he intends to sign.[147] Whether or not he intended to sign a particular document is again a question of proof, the standard of which will depend on the type of document.

The standards are intended to be very flexible to allow for changes in technology.

Part 2 of the UECA seeks to clarify the common law rules of contract by establishing rules for particular kinds of communications, including:

- the formation and operation of contracts, (particularly where there is no human intervention, the "electronic agent" example);
- the effect of using automated transactions, (the "shrink wrap" clicking on an icon example);
- the correction of errors when dealing with a computer at the other end of the line (the electronic mistake); and
- deemed or presumed time and place of sending and receiving computer messages (the when and where of contract formation).

The UECA is similar to Bill C-6 in authorizing governments to use electronic technology to deliver services and communicate with citizens. The UECA, like the federal legislation, clarifies how individuals can deal with the government electronically (although

---

147 UECA section 10.

in this case, the provincial government) but also deals with rights between private parties and the effect of electronic communications on those rights.

On December16, 1999 the Province of Saskatchewan became the first to introduce e-commerce legislation based on the UECA. That legislation, entitled *The Electronic Information and Documents Act*, is currently being debated in the Saskatchewan Legislative Assembly. No other Canadian province has introduced similar legislation.

(e) **International Conventions**

An agreement for the sale of goods between a person in Canada and a party in another jurisdiction may require the consideration of international conventions dealing with the sale of goods. The first of such conventions to review is the *United Nations Convention on Contracts for the International Sale of Goods*[148] (also known as the "Vienna Convention") which came into force on January 1, 1988, after it had received the necessary number of ratifications.[149] Canada, as a consequence of its ratification, has incorporated the Vienna Convention into its laws both federally,[150] and in the common law provinces and territories.[151]

The Vienna Convention and the statutes promulgated under that Convention apply to contracts for the sale of goods between commercial parties where the parties have

---

148 Reprinted at 19 I.L.M. 668 (1980).

149 *Symposium on Vienna Convention on Contracts for the International Sale of Goods* (1988) 21 Cornell Int. J.J. 419.

150 S.C. 1991, c.13.

151 S.A. 1990, c. I-6.8; S.B.C. 1990, c. 20; S.M. 1989-90, c.18 – c. S11; S.N.B. 1989, c. I-12.21; R.S.N. 1990, c. I-16; S.N.S. 1988, c. 13; R.S.O. 1990, c. I.10; R.S.P.E.I. 1988, c. I-6; S.S. 1990-91, c. I-10.3; R.S.N.W.T. 1988, c. I-7; S.Y. 1992 1992, c. 7.

places of business in differing signatory states.[152] The Vienna Convention does not, however, apply to the validity of the contract itself or any of its provisions,[153] the effect of a contract on the property in the goods,[154] nor does the Vienna Convention address jurisdictional issues. All of these issues remain to be addressed according to the applicable conflict of law rules in the jurisdiction where the matter is being decided.

A second, and perhaps more significant international convention as it relates to jurisdiction, is the *Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters*[155] (also known as the Brussels Convention). This Convention deals with the issue of jurisdiction to adjudicate and also covers enforcement of foreign courts' judgments.

According to this Convention, the general rule is that persons domiciled in a contracting state shall, whatever their nationality, be sued in the courts of that state.[156] There are some exceptions to this general rule that will in certain circumstances allow the plaintiff to choose a jurisdiction other than the defendant's residence. By way of example, in matters relating to a contract, the plaintiff can choose to sue either in the place where the

---

152 Art. 1. Also, the Vienna Convention does not apply to: contracts for the sale of goods bought for personal, family or household use; sales by auction, sales of electricity, sales of stock, shares, investment securities, negotiable instruments or money, or to sales of ships, vessels, hovercraft or aircraft; contracts for the supply of goods to be manufactured or produced where the party ordering the goods undertakes to supply a substantial part of the materials necessary for such manufacture or production; contracts in which the preponderant part of the obligations of the supplier of goods consists in the supply of labour or other services.

153 Art. 4(a).

154 Art. 4(b) except to the extent expressly provided in the Convention.

155 *Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters*, 1972 J.O. (L 299) 32, reprinted 29 I.L.M. 1417.

156 Art. 2.

contract is to be performed, or, if different, the domicile of the defendant.[157] For tort claims, Article 5.3 of the Brussels Convention designates "the courts for the place where the harmful event occurred." In torts on the Internet, however, there may be more than one such place. If, for example, a musical recording is posted, without permission, on a website in England, the infringer has made the work available for downloading everywhere there is access to that website. The courts of each of the place of initiation and the places the harm is caused are all competent under section 5.3, provided they are each Contracting States.

Contrary to U.S. and Canadian law, having a "real and substantial connection" with the state or 'doing business' in that state is not a permitted basis for the exercise of jurisdiction. Residence and domicile are the key (but not exclusive) factors.

The Contracting States to the Brussels Convention only include members of the European Economic Union and not Canada or the United States. The Brussels Convention's limitations on the jurisdiction of E.U. courts do not govern litigation between persons domiciled in the E.U. and non-E.U. domiciled defendants. Rather, the domestic civil procedure and conflicts rules of each national forum apply.[158]

Canadian and U.S. e-commerce companies should address the issue as to whether their activities over the Internet will bring them within the purview of the Brussels Convention. For example, if their company has servers located in Europe or if the company has a distribution centre located in Europe to deliver goods purchased over the Internet, these factors may be sufficient to trigger the jurisdictional rules imposed by the Convention.

---

157 Art. 5(1).

158 *Canadian Conflict of Laws*, 4th ed. (Vancouver: Butterworths, 1997), J.G. Castel at 7.

(f) **Payment**

If a supplier is selling goods and services over the Internet and being paid by the use of a credit card, few issues are involved with such a transaction. If, on the other hand, the transaction is one between businesses, involving invoicing for the goods or installment provisions, interest will likely be charged as part of granting the credit. There are numerous federal and provincial laws dealing with interest charges and credit disclosure requirements. Ensuring that the agreement between the parties contains an enforceable jurisdictional clause, and a choice of law clause will be vital but, according to local legislation, may not be determinative as to which jurisdiction's laws will apply to the contract of sale.

(g) **Data Collection – Privacy**

Data protection measures vary considerably from one jurisdiction to another and often from one business sector to another. Consumers frequently deal directly on-line with vendors located in countries where privacy laws and expectations differ from their own. Whose data protection laws and which enforcement mechanisms will govern the collection and use of personal information?

Website privacy policies in the U.S. are largely based on a sectoral approach that relies on a mix of legislation, regulation and self-regulation and is often based on new and rapidly evolving rules and practices broadly described as "fair information practices".[159] The primary factor in both the tort area and the emerging legislation is that of informed

---

159 S. Killingsworth, *Minefields Hopscotch: Introduction to Web Site Privacy Law* published by the Law News Network's Tech Law Center found at http://www.lawnewsnetwork.com/practice/techlaw/papers/lawfirm/A8555-1999Oct29.html

consent. Typically, consent is required for the collection of personal information and the subsequent use or disclosure of that information.

Apart from legislative and regulatory schemes, the most relevant body of law related to website privacy is the tort of invasion of privacy, which occurs through public disclosure of private information. To succeed, the plaintiff must show that (i) the disclosure of such information would be highly offensive or humiliating to a reasonable person, (ii) is of no legitimate concern, and (iii) the disclosure is disseminated widely enough to be considered public knowledge. Unless the information being collected is extremely sensitive, in most instances the normal collection of information for marketing purposes would be unlikely to attract liability.

"Fair information practices" include such practices as the provision of notice as to what data is being collected and for what purposes, the ability to choose whether or not to permit the collection of data, access by the consumer to the information being collected, measures to ensure the security and integrity of the information and appropriate means for enforcement. These practices were first articulated in 1973[160] and subsequently formed the basis of the guidelines adopted by the Organization for Economic Cooperation and Development in 1980,[161] and with further refinements, forming the basis of the EU Privacy Directive.

---

160 The Department of Health, Education and Welfare, Records, Computers, and the Rights of Citizens (1973).

161 OECD, *Guidelines for the Protection of Personal Data and Transborder Flows of Personal Data* (1980).

In the U.S., the Federal Trade Commission[162] has enforcement power over "deceptive acts or practices", but does not have the authority to require privacy policies or regulate their content. Their enforcement power can be invoked to ensure a website operator complies with the representations made to the consumer as to how their information will be used.

The *Children's On-line Privacy Protection Act,*[163] enacted in 1998, applies to commercial websites targeted to children or those that collect information about children who are 12 years of age and under. It codifies the "fair information practices" starting with the requirement to post a privacy policy that includes notice of:

1. who is collecting the data;
2. what data is being collected
3. how the data will be used;
4. to whom the data may be disclosed; and
5. the consequences of refusing to give the information.

The Act provides that there must be prior "verifiable consent" to the collection, maintenance and disclosure of information about children. Notwithstanding that the parent chooses to allow the collection of data by "opting-in", there remains an ongoing right to prevent further use or collection of information from their child. Further, parents have access to the information being stored about their children and the operator must take

---

162 15 U.S.C.A. section 41 et seq.

163 *The Children's Online Privacy Protection Act,*15 U.S.C.A. section 6501 et seq.

reasonable measures to protect the security of such data and ensure its integrity and accuracy. Rules for content and placement of the privacy policy will be defined in the FTC regulations.

Currently there is no similar legislation that applies to the collection of data from adults or children over the age of 12.[164]

The European Union Directive

The European Union ("EU") Member States, with a view to effecting greater harmonization of the data protection laws, passed Directive 95/46/EC relating to the protection of individuals with regard to the processing of personal data and the free movement of such data (the "EU Data Protection Directive").[165] The EU Data Protection Directive was adopted in 1995 and was to be implemented by the Member States by October 1998.

The EU Data Protection Directive regulates the "processing" (defined to include anything that can be done with data, from collection to deletion) of "personal data" (data about an identified or identifiable individual) either by automated means or as part of an organized filing system for commercial purposes about European citizens to other countries that lack 'adequate' protection of privacy.

---

164 There are some exceptions in specialized legislation dealing with consumer reports used for purposes such as credit or insurance underwriting and employment decisions (the *Fair Credit Reporting Act*, 15 U.S.C.A. section 1681 et seq.), the *Electronic Communications Privacy Act* (18 U.S.C.A. sections 2510-2522, 2701-2711) which applies to the monitoring or disclosure of e-mails or private discussions by a site that provides those services, and some privacy laws relating to medical information.

165 Directive of the European Parliament and of the Council on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data, October 1995. Available at http://www2.echo.lu/legal/en/dataprot/directiv/directiv.html.

The Data Protection Directive raises some interesting issues relating to jurisdiction. Firstly, if U.S. companies collect the data on computers located in the U.S., it is unlikely that Member States of the EU can exert any control over the use of information collected about European residents. If an EU Member takes action in their country against a U.S. company for failure to comply with the EU Data Protection Directive, that country's right to take jurisdiction over the U.S. company will no doubt be at issue along with the question of which laws apply to this collection of data.

For example, Article 25 Principle 1 states that the Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with, the national provisions adopted pursuant to the other provisions of the EU Data Protection Directive, the third country in question ensures an adequate level of protection. Principle 2 requires that the "adequacy of the level of protection afforded by a third country shall be assessed in light of all the circumstances surrounding a data transfer operation or set of data transfer operations; and particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

The EU Data Protection Directive also provides that even if the third country does not have adequate data protection measures in place, a transfer of personal data may

still take place on condition that the data subject has given his consent unambiguously to the proposed transfer.[166]

Some concerns raised about the impact of the EU Data Protection Directive include:[167]

1. "The Europeans are not going to tolerate the existence of 'data havens'" that operate beyond the reach of the Directive;
2. "[T]he initial determination of 'adequacy' will remain with the national data protection agencies."
3. "…once these issues enter the [European] Commission they are likely to be influenced by wider political and economic concerns."
4. "… will 'adequacy' just be measured against the principles of the Directive or also against the methods of enforcement and oversight?"
5. "*…neither the supervisory authority nor the data controller has the power to scrutinize the processing of personal data in another jurisdiction*, nor can they be fully satisfied that data subjects can exercise their privacy rights." [emphasis added]

All multinational firms now operating in Europe with a U.S. presence may find it necessary to alter their data collection and processing standards in response to the perception that U.S. privacy protection is less than adequate. As a result, the EU and the U.S. have been negotiating "Safe Harbor" principles that U.S. companies could adopt to ensure

---

166 Article 26 Derogations 1.

167 C.J. Bennett and C.D. Raab, *The Adequacy of Privacy: The European Union Data Protection Directive and the North American Responses*, *The Information Society*, vol. 13, 1997 at 245-263.

continued access to consumer data from Europe. These principles resemble the FTC 'fair information practices" with greater ability to "opt-in" before specified information is gathered and the ability to "opt-out' of some uses of the information. If an organization adopts these principles, publicly declares their adherence to these principles, and the organization is subject to the jurisdiction of the FTC or another government body with powers to take enforcement action in cases of deception or misrepresentation, the organization privacy policies will be considered 'adequate' for purposes of the EU Directive.[168] If a U.S. based organization collecting data in Europe does not voluntarily choose to comply with the safe harbor principles, these companies may find that information about European customers cannot be shipped to the U.S. for processing.

Some companies operating internationally may be able to satisfy the requirement by demonstrating that voluntary practices they have put in place meet the necessary 'adequacy' test or that they have obtained the unambiguous consent of the person whose information is being processed.[169] It has been argued that self-regulation by the industries and firms most likely to be affected is a more positive approach considering that the U.S. has no appetite for the kind of across-the-board regulatory approach now prevalent in Europe.[170]

---

168 *Summary of the Main Operative Provisions of a Possible Decision on the Basis of Article 25.6 of the Data Protection Directive Concerning the U.S. 'Safe Harbor'* found at www.ita.doc.gov visited January 2, 2000.

169 *Draft International Safe Harbor Privacy Principles Issued by the U.S. Department of Commerce*, November 15, 1999, found at www.ita.doc.gov visited January 2, 1999.

170 P.P. Swire and R.E. Litan, *Avoiding a Showdown Over EU Privacy Laws*, Brookings Policy Brief Series No. 29, Brookings Institution, February 1998. Accessed from http://www.brook.edu/comm/policybriefs/pb029/pb29.htm on January 2, 2000.

Canadian companies that process data relating to European customers and employees in Canada which comply with the guidelines set out in the proposed Bill C-6, may not have the same concerns with the EU Data Protection Directive.

Apart from Quebec, which has a data protection law based upon the French model,[171] Canada has, until recently, relied on self-regulation for commercial collection, processing and use of personal information. Partly spurred by the EU Data Protection Directive, Bill C-6, the *Personal Information Protection and Electronic Documents Act* was passed by Parliament October 1999.[172] The first part of the proposed Act establishes a right to the protection of personal information (such as race, color, age, marital status, religion, education, blood type *inter alia*.) collected, used or disclosed in the course of commercial activities in the private sector. Commercial activity is any activity of a commercial character including sales, purchases, exchanges and barters excluding some activities in the health sector and information collected solely for journalistic, artistic or literary purposes.

The Bill further provides for a Privacy Commissioner to receive complaints concerning contraventions of the principles, conduct investigations and attempt to resolve such complaints. Unresolved disputes relating to certain matters can be taken to the Federal Court of Canada for resolution.

Protection of this information is accomplished by requiring organizations to comply with the obligations in the Canadian Standards Association's (CSA) Model Privacy

---

171 *Quebec Act Respecting the Protection of Personal Information in the Private Sector*, 1993, Bill 68 (1993, chapter 17), National Assembly of Quebec, Second Session, thirty-fourth Legislature.

172 The Bill was passed by the Senate in December, 1999. The Bill, passed by the Senate, includes an amendment to define personal health information and to delay implementation of the Bill to such information for one year. As a result, the Bill must be reconsidered by the House of Commons.

Code, which is attached as a schedule to the Bill. This Code was established following input by most interested sectors, including consumer advocacy groups and is modelled on the OECD Privacy Guidelines adopted in 1981.[173]

Following a one year transition period, the Act will apply to the federally regulated private sector, namely telecommunications, broadcasting, banking and interprovincial transportation, in respect of employee and customer information. It will also apply to organizations that trade in personal information across interprovincial and national borders such as credit reporting agencies, credit card companies and website operators operating interprovincially or internationally. After three years the law will apply to all commercial activity, including activities that are provincially regulated unless the province passes a law that is substantially similar to the Bill, in which event the province's legislation will govern those organizations and activities covered by the provincial law.

The obligations that the organizations are required to meet are contained in ten principles which relate to accountability, identifying purposes, consent, limiting collection, limiting use, disclosure and retention, accuracy, safeguards, openness, individual access and challenging compliance. These principles apply to the collection of "personal information" which means information about an identifiable individual in any form[174] and applies to information in the possession or custody of the organization, including information that has been transferred to a third party for processing.[175] The primary principle in the

---

173 *Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data*, Organization for Economic Cooperation and Development, 1981, Paris: OECD.

174 Bill C-6, s.2 (1).

175 Bill C-6, Schedule 1, section 4.1.3.

CSA's Model Privacy Code, however, is the requirement for companies to obtain an individual's consent when they collect, use or disclose the individual's personal information.

Jurisdictional difficulties arise which are similar to those experienced in the U.S. Given that so much personal information on Canadians flows to the U.S. where it is stored, processed, transferred and generally used beyond the jurisdiction of the Canadian government, there may be little comfort given to Canadians with the passage of the Bill into law.

It is still difficult to ascertain the residence of a website visitor or e-mail addressee, and it is difficult for vendors to restrict their campaigns geographically. Currently, the courts appear to be restricting the assumption of jurisdiction over website operators that do not deal directly with consumers in the forum. However, data can occasionally be collected merely from a visit to a website located in another country and might be used for e-mail solicitations even if the consumer does not make a purchase. If the website operator in fact uses the information gathered to make e-mail solicitations, this may be viewed in the U.S. to be sufficiently interactive to constitute "minimum contacts" or to create a "real and substantial connection" in Canada. The chances are even greater if there is any active or extensive data collection from website visitors or efforts by the website operator to contact them directly. Thus, unless the website operator makes an effort to identify the residence of the consumer, and to comply with that state or province's privacy laws, the operator may become subject to jurisdiction in Canada, or elsewhere, for data protection violations.

There is currently no jurisdictional jurisprudence dealing with data protection in Internet cases. A violation of data protection laws may not normally result in substantial

monetary damages and the cost of litigation should keep most consumers from resorting to the courts, except in extreme cases of abuse.

The U.S. has, as a matter of policy, restricted their legislation to very specific areas.[176] Website operators in Canada that are actively collecting data from Canadian residents and are transferring that data interprovincially or internationally, would be well advised to comply with the proposed Bill C-6. Alternatively, the organization may wish to consider locating their computers in, and operating from servers located in, the U.S. where the privacy laws are, at the least, less restrictive and in some areas non-existent.

B. **Special Classes of People**

(a) **Consumer Transactions – Advertising**

Advertising on the Internet introduces legal risks for the e-commerce entrepreneur. Since content on-line can be accessed by potential customers worldwide, the potential for international and multi-jurisdictional liability arises.

The following fact situation is useful in illustrating issues arising from advertising on the Internet.

StereoCo, a Vancouver based company, manufacturers and markets stereo components to brokers throughout Canada and the U.S. who retail the components to consumers. Occasionally, StereoCo will deal directly with the consumer, but usually the contractual nexus is between the retailer and the consumer. Retailers have defined territorial sales areas.

StereoCo operates a website to describe the benefits of its products. A toll-free number is given to provide additional information. The website also describes any promotional items that StereoCo is marketing at a discount and is generally used as an advertising tool for its products. A consumer orders a pair of speakers manufactured by StereoCo from her local retailer and has them delivered to her home in Oregon. Music

---

176 See, for example, the federal *Children's Online Privacy Protection Act*, 1998 and recent "anti-spam" laws in individual states.

delivered over the speakers is highly distorted contrary to the representations on the website which claimed the clarity of the music delivered over the speakers was superior to Brand A. After discovering that such comparative advertising is not permitted by Oregon state law, the consumer registers a complaint with Oregon consumer affairs department.The state applies to an Oregon court for an injunction and damages against StereoCo.

In this example, the first issue to address is whether there is a connection between the website and the cause of action. In this case the conduct of StereoCo in placing comparison ads on their website is the very act that is the subject matter of the complaint and therefore the court only needs to find that StereoCo has sufficient contacts with that state to indicate that they have purposefully availed themselves of the privilege of conducting activities in the forum state, thereby invoking the benefits and protection of its laws.

As previously discussed, the preponderance of case law in the U.S. would suggest that something more than a passive website advertisement is required for the local court to assume personal jurisdiction. Moreover, unless the defendant's advertisements were specifically directed to that state, *IDS Life Ins. Co.*[177] would hold that such general advertising is not the type of 'purposeful activity' related to the forum that would make the exercise of jurisdiction fair, just or reasonable. However, a local court may look to other factors unrelated to the activity on the website to find other examples of 'purposeful activity' as in the cases of *Heroes, Inc. v. Heroes Foundation*[178] and *Blumenthal v. Drudge.*[179] The relationship between StereoCo and its retailers may be enough of a 'contact' to allow the court to claim jurisdiction.

---

177 *IDS Life Ins. Co. v. SunAmerica, Inc.*, 958 F.Supp. 1258 (N.D.Ill.1997).

178 *Heros, Inc. v. Heroes Foundation*, 958 F.Supp. 1 (D.D.C.1996).

179 *Blumenthal v. Drudge*, 992 F.Supp. 44 (D.D.C. 1998).

In the absence of such a relationship it is unlikely that Oregon courts would take jurisdiction over this matter.

StereoCo may, however, be exposed to liability under Canadian law. The federal *Competition Act*,[180] which was recently amended to meet the changing demands of the Canadian consuming public, contains broad prohibitions against making false or misleading representations to the public. Generally, this statute prohibits representations which are false or misleading in a material respect, whether such representations are made directly or indirectly.

It further prohibits:

1. False or misleading guarantees for the promise of replacement or maintaining an article where the form of the guarantee or warranty is material and misleading and there is no reasonable prospect that the warranty or guaranty will be carried out.
2. Misleading representations as to the price at which the article is ordinarily sold.
3. Double ticketing.
4. Certain multi-level marketing activities.
5. Bait and switch practices.
6. Contests which do not disclose the number and approximate value of the prizes or material information relating to the chances of success.

---

180 R.S.C. 1985, c. C-34, as amended.

The Act provides two avenues for combating misleading advertising. The first is criminal, and is detailed in the misleading advertising provisions. The second involves a civil process whereby the Competition Bureau counters misleading advertising by obtaining corrective redress from the courts, without criminal sanctions.

In comparing its products with those manufactured by Brand A, StereoCo may also be exposed to an action in Canada under section 7(a) of the *Trade-marks Act*[181] if the advertisement is found to contain false or misleading statements which tend to discredit the targeted competitor's business.

Countries throughout the world have varied regimes to protect their consumers and they will not easily relinquish their sovereignty in the application of those laws when their citizens are adversely affected by a transaction conducted on the Internet. It would be reasonable to assume that the threshold for foreign courts to assume jurisdiction in such consumer transactions will be low.

C. **Special Classes of Products**

(a) **Adjudicatory and prescriptive jurisdiction**

The ability of the forum to apply its state or federal laws to the dispute or the person depends on, *inter alia*, whether the application or use of that law conflicts with established principles of international law, international comity and foreign relations.

As previously indicated, one of the basic tenets of international law is that sovereign states have exclusive jurisdiction in their own territory to control both the residents of that jurisdiction and the rights to property found within that state. Briefly, applying the

---

181 *Trade-Marks Act*, R.S.C. 1985, c. T-13, as am. S.C. 1990, c. 14; c. 20; 1992, c. 1; 1993, c.15; c. 44; 1994, c. 47; 1995, c. 1; 1996, c. 8.

principles of territoriality, a country has jurisdiction to prescribe law when one of the following factors is present:

1. The conduct takes place wholly or in "substantial part" in the country's territory;
2. The question is the status of persons, or interest in things, found in the country's territory;
3. When the activities, interests, status or relations of the country's nationals both within and without the territory of the country are affected; or
4. There is conduct outside the country that is directed against the security or certain other national interests of the country.[182]

Even if one of these factors is present, an overriding test of reasonableness is applied which takes into account the consideration for the interests of other states.[183] Generally, courts in both the U.S. and Canada look to physical presence in the country or contacts with their country as the principal basis for both prescriptive and adjudicatory jurisdiction, however the "effects doctrine" has gained popularity with respect to criminal law, trademarks and securities regulation.[184] Canada requires a "real and substantial

---

182 *Restatement of the Law Third, Restatement of the Law, The Foreign Relations Law of the United States* (1987) section 402. These rules represent a fairly accurate summary of the general principles applied in Canada.

183 *Restatement of the Law Third, Restatement of the Law, The Foreign Relations Law of the United States* (1987) section 403.

184 *Panavision Intern., L.P. v. Toeppen*, 938 F.Supp. 616 (C.D.Cal.1996) at 621.

connection" between the action and the forum, recognizing the principles of comity and *forum non conveniens* to balance the interests of the parties with the interests of the forum.[185]

The Supreme Court of Canada in *Libman v. The Queen*, [1985] 2. S.C.R. 178 considered the territoriality principle as it applies to criminal law. *Libman* involved a fraud charge under the *Criminal Code* where the accused conducted activities in several countries, including Canada. In reviewing the history of English and Canadian law as it relates to criminal offences, La Forest J. stated:[186]

> [T]he territorial principle in criminal law was developed by the courts to respond to two practical considerations, first, that a country has generally little direct concern for the actions of malefactors abroad, and secondly, that other states may legitimately take umbrage if a country attempts to regulate matters taking place wholly or substantially within their territories. For these reasons the courts adopted a presumption against the application of laws beyond the realm...

The principle has not, however, been so rigidly applied. If a person's actions abroad have an unlawful consequence within the state, the Court acknowledged that the control of such activities and the protection of the public are legitimate purposes for the criminal law. The principle of international comity has traditionally been viewed as a consequence of the territoriality principle, limiting a country's authority to exercise jurisdiction over cases that involve persons, interests, or activities of persons who are residents of other countries.[187] In discussing the applicability of comity to actions occurring outside the state which have unlawful consequences in the state, La Forest J. applied the

---

185 See *Hunt v. T&N plc.* [1993] 109 D.L.R. (4th) 16.

186 *Libman v. The Queen*, [1985] 2. S.C.R. 178 at 208.

187 *Canadian Conflict of Laws*, 4th ed. (Vancouver: Butterworts, 1997), JG Castel at 15-16.

reasoning of the House of Lords in *Tracy v. Director of Public prosecutions,* [1971] A.C. 537, a case involving a criminal charge of blackmail where the accused posted a letter in England to a woman in West Germany demanding money upon certain threats. La Forest described Lord Diploic's decision as follows:[188]

> In his view, if the facts alleged and proved constitute the offence charged, the only reason...for refusing to convict was to be found in the international rules of comity which must be presumed Parliament did not intend to break. But he interpreted comity narrowly to attempts to regulate conduct abroad and not in the United Kingdom. As he put it, at p.561:
>
> It would be an unjustifiable interference with the sovereignty of other nations over the conduct of persons in their own territories if we were to punish persons for conduct which did not take place in the United Kingdom and had no harmful consequences there. But I see no reason in comity for requiring any wider limitation than that upon the exercise by Parliament of its legislative power in the field of criminal law.
>
> In particular he noted that comity did not prevent Parliament from prohibiting conduct in England that has consequences abroad. Nor did it give immunity to persons abroad for conduct there that has harmful consequences in England. He continued at pp. 561-62:
>
> There is no rule of comity to prevent Parliament from prohibiting under pain of punishment persons who are present in the United Kingdom, and so owe local obedience to our law, from doing physical acts in England, notwithstanding that the consequences of those acts take effect outside the United Kingdom. Indeed, where the prohibited acts are of a kind calculated to cause harm to private individuals it would favour of chauvinism rather than comity to treat them as excusable merely on the ground that the victim was not in the United Kingdom itself but in some other state.
>
> Nor, as the converse of this, can I see any reason in comity to prevent Parliament from rendering liable to punishment, if

---

188 *Libman v. The Queen*, [1985] 2. S.C.R. 178 at 195.

> they subsequently come to England, persons who have done outside the United Kingdom physical acts which have harmful consequences upon victims in England. The state is under a correlative duty to those who owe obedience to its laws to protect their interests and one of the purposes of criminal law is to afford such protection by deterring by threat of punishment conduct by other persons which is calculated to harm those interests. Comity gives no right to a state to insist that any person may with impunity do physical acts in its own territory which have harmful consequences to persons within the territory of another state. It may be under no obligation in comity to punish those acts itself, but it has no ground for complaint in international law if the state in which the harmful consequences had their effect punishes, when they do enter its territories, persons who did such acts.

The limits of comity as it applies to a state's right to prescribe conduct, is summarized by La Forest, as follows:[189]

> As I see it, all that is necessary to make an offence subject to the jurisdiction of our courts is that a significant portion of the activities constituting that offence took place in Canada. As it is put by modern academics, it is sufficient that there be a "real and substantial link" between an offence and this country, a test well known in public and private international law...

La Forest J. also described the need to adopt an evolving, and broader, concept of comity:[190]

> Just what may constitute a real and substantial link in a particular case, I need not explore. There were ample links here. The outer limits of the test may, however, well be coterminous with the requirements of international comity.
>
> As I have already noted, in some of the early cases the English courts tended to express a narrow view of the

---

189 *Libman v. The Queen*, [1985] 2. S.C.R. 178 at 212.

190 *Libman v. The Queen*, [1985] 2. S.C.R. 178 at 213.

> territorial application of English law so as to endure that they did not unduly infringe on the jurisdiction of other states. However, even as early as the late 19th century, following the invention and development of modern means of communication, they began to exercise criminal jurisdiction over transnational transactions as long as a significant portion of the chain of action occurred in England. Since then means of communications have proliferated at an accelerating pace and the common interest of states have grown proportionately. Under these circumstances, the notion of comity, which means no more or less than "kindly and considerate behavior towards others", has also evolved. How considerate is it of the interests of the United States in this case to permit criminals based in this country to prey on its citizens? How does it conform to its interests or to ours for us to permit such activities when law enforcement agencies in both countries have developed cooperative schemes to prevent and prosecute those engaged in such activities? To ask these questions is to answer them. No issue of comity is involved here...[We should not be indifferent to the protection of the public in other countries. In a shrinking world, we are all our brother's keepers. In the criminal arena this is underlined by the international cooperative schemes that have been developed among national law enforcement bodies.

Stretching the limits of comity even further, the Supreme Court of Canada in *Tolofson v. Jensen*[191] declared that in actions involving tortious conduct, the law to be applied is that of the place where the wrongful activity occurred. This may not be the same place as where the effect (or damage) consequent to the activity occurred. It is likely, however, that a determination of where the damage is caused and where the activity takes place will each create links with the state that may be sufficient to meet the requirements of comity. If a defendant's conduct, whether criminal or tortious, occurred in a state, or had an effect in that state, it is probable that the state will assume jurisdiction over the person and also apply its laws, whether criminal or civil, to the conduct at issue.

---

191 *Tolofson v. Jensen*, [1994] 3 S.C.R. 1022, [1995] 1 W.W.R. 609, 120 D.L.R. (4th) 289.

(b) **The Example of Amazon.com**

Concerns about a Canadian company being haled into an overseas court because that conduct is illegal in that country can be illustrated by the recent lawsuit by the German government against Amazon.com for selling books containing information about Nazi's. Such activity is illegal in Germany.

German authorities clearly have the jurisdiction to prescribe that it is a crime to provide Nazi propaganda to the German population whether it is provided over the Internet or by other means. This flows from the basic principle of state sovereignty that gives every state the power and right to enact laws provided it does so within the guidelines of international law. This jurisdiction could have been limited by Convention, if Germany had entered into a Convention dealing with this issue, or by adhering to an international custom (if there was one) which limits this right.

It is also a well established principle that a state has the right to exercise adjudicatory jurisdiction over persons, property, acts or events occurring within its territory. This is subject to the principle of international comity described above. Germany has the right to prescribe what is a crime in Germany and to prosecute persons committing crimes in its territory. Whether or not German authorities have the right to punish persons who carry out this illegal conduct from another country is another question. Clearly, German authorities cannot arrest the president of Amazon.com in the U.S. or otherwise enforce its laws against property in the U.S. without violating another state's sovereignty. The U.S. would have to agree to extradite him to Germany or the president would have to be foolish enough to land on German soil.

The concern of Internet operators is that it is presently unclear where the crime is committed when the activity complained of occurs on the Internet. As indicated above, a state has jurisdiction to prescribe acts committed in their territory. Also, it must be remembered that a state has jurisdiction over acts commenced in another state but consummated or completed in their territory and also over acts which have harmful effects on the economic or social order inside their territory.[192] This puts the operator of Amazon.com at risk that they may be exposed to prosecution and extradition in a foreign country for crimes committed over the Internet.

(c) **Gambling**

The business of gambling over the Internet is growing at an exponential rate. Some 200 companies around the world operate at least 700 on-line casinos. Roughly 14.5 million players spent $1.2 billion on virtual gaming in 1999, and the industry projects revenues of more than $3 billion by the year 2000.[193] Federal legislators in the U.S. want to ban the activity through a proposed Act, the *Internet Gambling Prohibition Act*, that would bar gambling businesses from using the Internet to place or take bets. Most states already prohibit or control gambling within their jurisdiction and it is expected that legislators and the courts will take steps to 'protect their citizens' from the perceived evils caused by this activity.

---

192 *Starke's International Law*, (London: Butterworts, 1994), I.A. Shearer, at 187.

193 R. Eckstein, *Rolling the Dice: Internet Gambling foes bet on odd coalition. But will it pay off?*, Legal Times, March 14, 2000 found at http://www.lawnewsnetwork.com/practice/techlaw/news/A18529-2000Mar13.html.

One such example can be found in the case of *State of Minnesota v. Granite Gate Resorts, Inc.*[194] In this case, the state brought an action alleging deceptive trade practices, false advertising and consumer fraud over the Internet against the defendant who advertised an on-line casino in Belize. The complaint stated that the website advertised the fact that gambling on the Internet was lawful, whereas in Minnesota it was not. The defendant had an advertisement on its website for a service called "WagerNet" to be provided by a related company in Belize. The advertisement encouraged people to sign up for an e-mail mailing list that would advise those on the list when the electronic betting service became available. The advertisement also encouraged visitors to contact the company directly, through its toll-free number, for additional information while warning users that they should consult with their local authorities to determine the legality of placing bets by telephone with an off-shore betting facility before using WagerNet.

Although the defendant maintained that it had never entered into any contract in Minnesota or collected any money from a resident of Minnesota, the state argued that the web pages were accessible in Minnesota and therefore the defendant was 'carrying on business' in the state for the purposes of jurisdiction.

In assessing whether the defendant had established sufficient minimum contacts with the state for the court to assume jurisdiction, the Court of Appeals for Minnesota adopted a five-factor test :

1. The quantity of the contacts with Minnesota;

2. The nature and quality of the defendant's contacts;

---

194 *State of Minnesota v. Branite Gate Resorts, Inc.*, 568 N.W. 2d 715 (Ct.App.) Minn. 1997), *aff'd*, 576 N.W. 2d 747 (Minn. 1998).

3. The connection between the cause of action and the defendant's contacts;

4. The state's interest in providing a forum;

5. The convenience of the parties.

The court found that by merely advertising the gambling services on the Internet the defendant had demonstrated a clear intention to solicit business from all states, including Minnesota. This was evidenced by phone calls from residents of Minnesota to the defendant on their toll-free line, the addition of residents to a mailing list, and the number of hits on the website originating from Minnesota. The court noted that the "[d]efendants keep track of who is accessing their website, and therefore know that Minnesota computers are accessing them."[195] Additionally, there was a connection between the cause of action and the defendant's advertisements on the website. The convenience of the parties was resolved by finding that the state's interest in enforcing its consumer protection laws was greater than the inconvenience to the defendant to defend against the suit in Minnesota. As a result, the court was able to find that the defendant had purposefully availed itself of the protections and benefits of doing business in Minnesota to such an extent that the action by the state does not offend traditional notions of fair play and substantial justice. Although minimal, the level of interactivity between the defendant and the state's residents was held to be sufficient enough to warrant the exercise of personal jurisdiction.[196]

Often, in the consideration of jurisdictional issues, questions of adjudicatory jurisdiction are intermingled with questions of prescriptive jurisdiction. In areas of consumer

---

195 *State of Minnesota v. Granite Gate Resorts, Inc.*, 568 N.W. 2d at 719.

196 See also *Thompson v. Handa-Lopez* 998 F. Supp. 738 (W.D. Tex. 1998) however this was a dispute based on contract, and not one with the state.

protection, such as securities regulation, and certain quasi-criminal activities, such as gambling, the courts often fail to distinguish between the two. A positive finding in either area seems to result in the automatic application of the other.

The forgoing would suggest that in circumstances where the state has an interest in the litigation for the purposes of 'protecting its residents', the test for meeting the minimum contacts requirement is a much lower standard than in civil litigation between two private parties. Moreover, it was assumed by the court that once adjudicatory jurisdiction was appropriate, the state's consumer protection laws could therefore be applied to the defendant's conduct. Once that lower standard has been met, it is reasonable to expect the courts will apply their laws to the conduct under review.

(d) **Professional Services**

Services that are not regulated by either a professional body or by a governmental equivalent raise few new issues for jurisdictional analysis and the evolving jurisdictional framework can be effectively applied to delivery of those services. The same holds true for a civil action against the provider of a professional service. Assuming a court has found they should take jurisdiction over the issue and the parties, when more than one state, province or country has prescribed law that could reasonably be applied to the conduct at issue, courts are required to engage in conflict of law analysis, choosing which law to apply. In the United States, this is typically based on an assessment of the jurisdiction with the most significant relationship to the parties, the activities conducted and the weightiest

state interests at stake.[197] In Canada, this is also generally the case except in tort cases where a strict *lex loci delicti* (the place where the tortuous activity occurred) rule is applied.[198]

Like gambling, however, the sale of professional services over the Internet attracts the public regulatory policies and powers of sovereign states and highlights the difficulties encountered when applying traditional jurisdictional analysis to the provision of these services in cyberspace. At issue is the ability of regulatory bodies to govern who provides the services as well as what services may be provided. In other words, when will a state assume "prescriptive jurisdiction" over the person as compared with "adjudicatory" jurisdiction.

The tendency of countries is to assert jurisdiction over any health care related activity affecting their citizens and not defer to the health care laws that protect consumers in other countries. In the future, as delivery of medical care over the Internet advances, greater attention will likely be paid to the jurisdictional issues raised in this area.

(e) **Securities**

A significant issue raised by the use of the Internet is whether offerings posted on a website, without more, might be subject to the securities regulations of every state, province or country from which they are accessible.

---

197 *Restatement of the Law Third, Restatement of the Law, The Foreign Relations Law of the United States* (1987) section 402 -3.

198 This rule, most recently articulated by the Supreme Court of Canada in *Tolofson v. Jensen*, [1994] 3 S.C.R. 1022 diverges from the 'most significant relationship' test in United States law, which is less exclusively based on territorial locus. This test also conflicts with the increased flexibility mandated by the Supreme Court when dealing with jurisdictional issues. In *Hunt v. T&N plc.* [1993] 109 D.L.R. 94th 16 (S.C.C.) the Court remarked on a need for "greater comity...in our modern era when international transactions involve a constant flow of products, wealth and people across the globe," and further held that "jurisdiction must ultimately be guided by the requirements of order and fairness, not a mechanical counting of contacts and connections." *Hunt v. T&N plc.* [1993] 109 D.L.R. 94th 16 S.C.C. Q.L., at para 53 and 58.

The mere posting of or the existence of an offering on the Internet alone should not be sufficient evidence that the offer is specifically "directed" to persons in every state and province. In fact it may not be intended that the offering be sold in any but a few specified states. Accordingly, unless an offer to sell securities is directed to residents of the forum state, either directly, by means of e-mail, telephone, or regular mail, or indirectly, by less clear means, or an order based on that general offering is accepted from the forum state, jurisdiction should be declined. There is, however, the desire of the state to 'protect the public' from those persons providing access to unregulated services on the Internet.

In order to reconcile technology, practicality and due process, the North American Securities Administrators Association (NASAA), a voluntary organization established in 1919 to protect investors, became the first super-regulatory entity to adopt a jurisdictional policy that would facilitate e-commerce in securities. The NASAA adopted a model rule, under which states will generally not attempt to assert jurisdiction over an offering if the website contains a disclaimer essentially stating that no offers or sales are being made to any resident of that state, the site excludes such residents from access to the purchasing screens, and, in fact, no sales are made to residents of that state.[199]

In Canada, the distribution of securities is regulated provincially. In addition, the provinces have jurisdiction over provincially incorporated companies. Until recently, Canada had little case law dealing directly with the extraterritorial reach of its securities laws beyond general jurisdictional principles. Although there has been much discussion in recent

---

[199] Model NASAA Interpretive Order and Resolution posted at www.nasaa.org/bluesky/guidelines/resolu.html. A majority of states (32 as of late 1999) have adopted the resolution and a further 16 stated they would adopt the resolution.

years about the possibility of a uniform law throughout the provinces, each province still has its own regulatory scheme and registration requirements.

Effective January 1, 2000, the securities commissions in all provinces in Canada adopted a policy proposed by the Canadian Securities Administrators, entitled "Trading in Securities Using the Internet and Other Electronic Means"[200] which indicates that each province will follow a jurisdictional policy similar to that of NAASA and the SEC in the United States. Applying a two-fold test, each province's policies would deem that its securities laws apply when either the person making a communication or the person to whom a communication is directed is located in that province. Like the NAASA approach, provincial regulators would not attempt to control sites which, at the outset, expressly exclude sales within that province or directs the communication exclusively to other, specified jurisdictions.[201]

In provincial jurisdictions, the use of the Internet to promote the sale of securities would pose problems in light of the definitions of a 'trade' in securities which generally includes 'any acts in furtherance of a trade'. How this broad definition will be interpreted in the face of aggressive or passive solicitations on the Internet will generate significant public interest. A recent decision by the Alberta Securities Commission (ASC)[202]

---

200 National Policy 47-201 *Trading Securities using the Internet and Other Electronic Means*, found at www.albertasecurities.com/pdfs/instruments/np47-201.pdf.

201 Section 2.2, National Policy 47-201 *Trading Securities using the Internet and Other Electronic Means*, found at www.albertasecurities.com/pdfs/instruments/np47-201.pdf.

202 Alberta Securities Commission decision on World Stock Exchange, Seto and Rusnak issued Feb. 15, 2000.

may shed some light on the restrictions securities regulatory bodies may impose relating to Internet activities.

The World Stock Exchange (WSE), one of the defendants, established a website, which was initially operated from a server in Edmonton and later moved to the Cayman Islands and finally to a server in Antigua. Information on how to list a company on the WSE and the fees charged for stock transactions finalized through the WSE could be found on their website. The Antigua website also contained a very bold statement respecting the jurisdiction of the Exchange:[203]

> The World Stock Exchange was incorporated and established in a manner that ensures that it does not fall under the Securities Regulations of any country. Only the regulations and policies of the World Stock Exchange control the listing of companies on the various Trading Boards of the World Stock Exchange.

The ASC disagreed with this statement. Section 52(1) of the Alberta Securities Act[204] states that "[no] person or company shall carry on business as an exchange in Alberta unless the person or company is recognized by the Commission as an exchange." It was argued by the WSE that the 'trading floor equivalent' of the WSE was located either in cyberspace, in Antigua where the correspondence is received, or in the Cayman Islands, where the transactions were completed and therefore the ASC was not carrying on business in Alberta.

---

203 Alberta Securities Commission decision on World Stock Exchange, Seto and Rusnak issued Feb. 15, 2000 at p.9.

204 S.A. 1981, c.S-6.1, as amended.

Although raised in the proceedings, the ASC found that all the cases and commentary in both the U.S. and Canada dealing with the question of personal jurisdiction over persons and claims involving the Internet had no relevance to the issue before the Commission. According to the ASC, their only concern was whether or not the WSE was carrying on the business of an exchange in Alberta, contrary to section 52(1) of the Act. The ASC assumed jurisdiction over the company even though it was incorporated in the Cayman Islands. The question of whether there was a real and substantial connection between the company, the action and the state was discussed, but only in the context of deciding whether the WSE had sufficient links with Alberta to justify the Commission in applying Alberta's laws to the defendants.

In addressing the question of whether Alberta's legislation should be applied to the activities of the WSE in Alberta the ASC followed *R. v. Libman*[205] in finding that all that was necessary for Alberta to apply its laws to the WSE was to find there was a "real and substantial link" between the offence and the state. The WSE was originally established in Alberta (although it was in that province for only days) and the directors were residents of Alberta who spent much of their time promoting the WSE to Albertans. The ASC found these activities were more than sufficient for Alberta to apply its laws. Moreover, the Commission found that it had a legitimate interest in applying Alberta law to the WSE "merely because its activities have unlawful consequences here".[206]

---

205 *Libman. v. The Queen* (1985), 21 C.C.C. (3d) 206, [1985] 2 S.C.R. 178 (S.C.C.).

206 Alberta Securities Commission decision on World Stock Exchange, Seto and Rusnak issued Feb.15, 2000 at p.38.

If the exchange was already regulated by another country, the ASC felt that different considerations would apply :[207]

> Quite different comity considerations might apply in a situation where section 52(1) was being used in an attempt to force an already regulated exchange to apply for recognition in Alberta. In that situation, there would be a major issue of comity because, in effect, we would be trying to superimpose Alberta's small-r regulation over the existing (and, presumably, somewhat different) small-r regulation of another jurisdiction. No exchange can operate lawfully if it is subject to inconsistent small-r regulation from two or more jurisdictions, so the principles of comity militate strongly against interpreting section 52(1) to capture any exchange whose activities do not raise significant public interest concerns in Alberta.

If the entities are not regulated by their home jurisdictions, the ASC encourages other jurisdictions to take a similar approach to protect the 'potential victims' of operations like the WSE that operate over the Internet: "There would be no purpose in having an elaborate framework of securities regulation to protect the public interest if the law permitted entities like the WSE to circumvent it all by using modern technology and communications to step beyond our jurisdiction."[208]

This decision gives support to the proposition that every state has prescriptive jurisdiction over activities on the Internet if that activity has some effect in the state which raise public interest concerns. The WSE made the mistake of having officers of the company physically spend time in Alberta encouraging people to list their companies on WSE's new 'cyberspace exchange'. This conduct alone would have allowed the Commission to assume

---

207 Alberta Securities Commission decision on World Stock Exchange, Seto and Rusnak issued Feb.15, 2000 at p.39.

208 Alberta Securities Commission decision on World Stock Exchange, Seto and Rusnak issued Feb.15, 2000 at p.38.

jurisdiction over the company and likely constituted enough conduct in Alberta to justify applying Alberta's securities laws to that conduct. It seems probable that when dealing with regulations that protect the public interests, there will be a very low threshold applied to the jurisdictional question. Such regulatory schemes will be treated in the same manner as criminal conduct, and the 'effects test' will likely be the primary test applied by the courts in determining prescriptive jurisdiction as the effect in the forum will be sufficient to establish the real and substantial link mandated by the Supreme Court in *Libman*[209]

(f) Products Carrying Copyright and Trademark Rights

(i) Copyright

Most works available on the Internet (messages, documents, music, photographs, drawings, videos, charts, databases) carry with them rights granted to the creator pursuant to federal copyright legislation. Copyright is purely a creation of statute. Accordingly, whether or not an author's rights have been infringed is totally dependant on whether the author was granted such rights under a particular statute. In the absence of international agreements to the contrary, copyright is strictly territorial in its application. Protection of a copyrighted work exists independently in each country according to the rights granted by that country. The protection afforded by each country is not the same.

As a result, if copyright in a sound recording is created pursuant to the *Copyright Act, Canada*, no rights accrue to the Canadian copyright holder to sue for an infringement which occurs beyond Canada's borders. If a person in Canada infringes the copyright granted to a person by the laws of another state, no action lies unless it also

---

209 *Libman v. The Queen* (1985), 21 C.C.C. (3d) 206, [1985] 2 S.C.R. 178 (S.C.C.).

infringes Canada's *Copyright Act*. [210] It has been suggested that there is no jurisdiction in Canadian courts to prevent infringement outside Canada and any action must be dealt with in the country[211] and pursuant to the copyright legislation in which the infringement takes place. Although the choice of law question is dealt with in Article 5(2) of the Berne Convention, which provides that copyright protection "shall be governed exclusively by the laws of the country where protection is claimed"[212], it is expected that the jurisdictional question will be dealt with in accordance with the 'minimum contacts' test in the U.S. and the 'real and substantial connection' test in Canada. Even if the court does assume jurisdiction, the question of which law to apply to the activity may be a difficult one.

In circumstances where the communication of the work takes place over the Internet, the decision as to which state has jurisdiction over the activity depends on a determination of where the infringement occurs - where the act of infringement takes place (posting to a website) or where it is received. The decision will be important to those holding copyright works disseminated over the Internet as it will be determinative of which country's laws establish the rights granted to the creator of the work and may also be significant in determining which country has jurisdiction to hear the question. The problem is that instant and simultaneous worldwide access to copyrighted works over a digital network

---

210 A Canadian copyright is generally given to foreign works if the author, at the time of making the work was a citizen or subject of, or a person ordinarily resident in, a treaty country. See s.5, *Copyright Act, Canada*. A "treaty country" is defined in s.2 to include a Berne Convention country, UCC country or WTO Member.

211 M. Hayes, "Content-Related Liability for Copyright Infringement on the Internet" in *The Cyberspace is Not a "No Law Land" - A Study of the Issues of Liability for Content Circulating on the Internet*, prepared for Industry Canada , Feb., 1997. Found at http://strategis.ic.gc.ca/nme.

212 See *Berne Convention for the Protection of Literary and Artistic Works of September 9, 1986*, art. (5(2), UNTS 221, 232.

fundamentally challenges territorial notions in copyright and often the determination of where the infringement takes place is unclear.

One author describes the problem this way:[213]

> Territoriality-based choice of law rules require that a court having been called to decide a multinational infringement case determines where potentially infringing acts occurred. If potentially infringing acts occurred in several countries, a court must apply the copyright laws of each country, even though they may characterize the relevant acts differently. If, for example, video tapes of a film were reproduced in one country without the rights holder's authorization and then sold and displayed in others, and the copies were then sold in several countries and also used to publicly show the film, the copyright law of the first country would govern the reproduction of the tapes, and the copyright laws of each other country would determine whether the imports, sales and public performances were lawful.
>
> Not surprisingly, applying strictly territorial choice of law rules to global digital networks creates formidable problems. The practicality of territoriality-based copyright choice of law rules is threatened by technology that allows single acts of use of a copyrighted work to have effects in several countries. It is no longer possible to neatly define where an 'act of use' triggering the application of a national copyright law occurred. A person providing access to a copyrighted work on a website, for example, frequently cannot control where viewers and listeners are located. She may have even less control over the location of computers involved in the transmission of copyrighted works. Acts of use that may fall within an exclusive copyright are not only committed by the access-providing person, but they may also be initiated by the end user who accesses the work. For end users, however, it may be equally impossible to identify the location of the source of the work they read and retrieve.
>
> Consider as an illustration the video tape example occurring in a digital environment. The film is uploaded in digital

---

213 A. Reindl *Choosing Law in Cyberspace: Copyright Conflicts on Global Networks,* 19 Mich.J. Int'l L. 799 at 806.

> format to a website on the GII [global information infrastructure], which possibly is located in another country, from where it can be retrieved by users anywhere in the world. In this scenario it becomes an almost impossible task to determine according to strictly territorial criteria under which copyright laws, importation rights, distribution rights, reproduction rights, or rights of display or performance may have been infringed.

If all countries offered the same standard of copyright protection, the need to determine where the infringing act occurred would be diminished. Important steps have been taken by the international community to meet this goal by implementation of the TRIPS[214] Agreement and two additional treaties. The World Intellectual Property Organization has drafted two treaties under its International Protection of Copyright and Neighbouring Rights Section, the WIPO Performances and Phonograms Treaty (WPPT),[215] which sets out principles on intellectual property rights for both the performers and the producers of recordings, and the WIPO Copyright Treaty (WCT)[216] which deals with computer programs and databases. Both treaties oblige Contracting Parties, as defined therein, to provide protection against tampering with technological protection measures (encryption) and rights management information (e.g. licensing, collecting and distribution of royalties).

The Copyright Treaty also grants to the owners of copyright in literary and artistic works the exclusive right to authorize any communication to the public, by wire or wireless means, including on-demand, interactive communication through the Internet. This would include making a work available, whether or not it is ever accessed. The mere

---

214 *Agreement on Trade Related Aspects of Intellectual Property Rights, Including Trade in Counterfeit Goods*, Dec. 15, 1993 (TRIPS).

215 Available at www.wipo.int/eng/dip/conf/distrib/95dc.htm.

216 Available at www.wipo.int/eng/dip/conf/distrib/94dc.htm.

provision of physical facilities for enabling or making a communication does not in itself amount to communication within the meaning of the Treaty.[217]

The *Performances and Phonograms Treaty* provides that the rights of reproduction, distribution rental and the right to make available are granted to performers who have fixed their performances in phonograms, and to the producers of these phonograms. Such rights also accrue to the performer or producer when the work is in digital form.

The *Digital Millennium Copyright Act* ("DMCA"),[218] which was recently put in to law in the U.S. was partially inspired by these two Treaties. In addition to limiting liability of Internet service providers, which is discussed elsewhere in this paper, the Act expands copyright protection for technological products and technological methods of protecting copyright works.

The DMCA establishes a new section of the *U.S. Copyright Act* (s.1201)[219] which prohibits the circumvention of technological measures designed to protect copyright works. Technological measures are of two kinds:

1. Those that control access to a work (an example is the measure used to scramble access to certain television stations). No one is permitted to

---

217 *Internet Law: A Practical Guide for Legal and Business Professionals*, Gatlan, Kratz and Mann, (Carswell: Toronto 1998) at 23.

218 Pub.L. 105-304, Oct.28, 1998, 112 Stat. 2860; 17 USCA sections 1201 - 1332.

219 *U.S. Copyright Act*, s. 103.

circumvent those measures or to import products whose primary function is to circumvent those measures.[220]

2. Technological measures that prevent copying and carrying on any other activity that is the exclusive right of the copyright owner (for example, a computer program that is encoded to prevent copying). Although the Act prohibits making, importing and supplying products to others whose primary function is to circumvent those measures,[221] there is no prohibition against the mere circumvention of copy protection as some copying is considered 'fair use' under the U.S. law.

There is a recent decision in the U.S. testing the provision restricting the development of tools that can be used to circumvent copyright control technologies. In *Universal Cities Studios Inc. v. Reimerdes,* S.D.N.Y., No. 00 Civ. 0277 (LAK), Jan. 20, 2000,[222] the defendants were enjoined from "posting on any Internet website, or in any other way manufacturing, importing or offering to the public, providing or otherwise trafficking in any technology, product, service, device, component, or part thereof" that "is primarily designed or produced for the purpose of circumventing…the protection afforded by the Content Scramble System (CSS)…"[223]

---

220 *U.S. Copyright Act,* s. 1201(a) and (b).

221 *U.S. Copyright Act,* s. 1202(b).

222 A similar case, but based on a violation of the plaintiff's trade secrets is *DVD Copy Control Association Inc. v. Mclaughlin,* No. CV-786804, Sup. Ct. Calif, January 21, 2000. The California state court granted a preliminary injunction against the defendants similar to the one granted in the *Universal Studios* case referred to above.

223 Westlaw at para 1.

The technology referred to is a software utility that was created by third parties (not the defendants) to enable Linux computers to utilize DVD drives and content. The independent programmers developed DeCSS because the commercial computer industry does not currently produce the necessary driver for the Linux operating system. Windows and MacOS do, by contrast, have the drivers to read and play DVD-ROMS. CSS was, of course, developed to prevent the copying of DVDs but it also prevents those operating Linux from playing a DVD on their computers. By reverse-engineering, the operating technology of CSS was revealed, allowing Linux developers to create the public domain DVD player.

Some concerns have been voiced[224] that the legislation is being used to control the market for DVD players. Without the ability to descramble the DVD, a manufacturer is unable to produce a DVD player to compete with that offered by the makers of the CSS technology, Matsushita Electric Industrial Co. and Toshiba Corp. It will be interesting to follow the development of this issue in the U.S. as it will no doubt have an impact on legislators in Canada that will be charged with implementing the terms of the Treaties into our legislation.

The DMCA also has provisions protecting copyright management information, as required by the Treaties.

Does Canada's *Copyright Act* meet the requirements of the WPPT and WCT Treaties? The wording of the Act is likely broad enough to apply to digital reproduction and transmission on the Internet. The rights afforded to holders of copyright are contained in section 3 of the Act and include the right to produce, reproduce, perform or publish a work

---

224 See Mike Godwin, *Courts Enjoin Sites That Publish DVD Decryption Software*, found at www.lawnewsnetwork.com/practice/techlaw/news/A14533-2000Jan28.html.

or any substantial part of a work, *in any material form whatsoever,* the right to communicate a work to the public by telecommunication and the right to license certain works. No provision has been made, however, to protect copyright management information nor is there any prohibition, similar to that contained in the DMCA, prohibiting the circumvention of measures that prevent access to or the copying of copyright material.

(ii) The Music Industry

The record industry is concerned that new technology, which permits CD quality sound to be transmitted by digital networks,[225] will play a key role in the pirating of copyrighted material over the Internet. By making a recording available on a site, millions of people around the world have the ability to download the song and record it for personal use.

When a musical work is 'communicated to the public' through the use of the Internet was recently scrutinized by the Canadian Copyright Board.[226] As this right is held by the owner of the copyright, one of the primary issues being discussed was where the infringement occurs which in turn impacts on whether Canada, through its copyright legislation, can impose tariffs on ISP's, website operators, or other persons in the chain of providing Internet services.

---

225 Jason Scott Alexander, in his article "MP3, Intellectual Property 0" (*National,* a publication of the Canadian Bar Association, Vol. 8, No. 8, Dec. 1999 at 8.) describes how MP3 (and, more recently, VQF) is used to compress the size of audio files at a ratio of approximately 11:1 while, to a great extent, maintaining audio quality. This technology allows recording companies to store full length CD's on small data capacity 'mini-discs' and, more importantly for the music industry, allows telecommunication firms to package voice and audio data to send along digital networks. Individual consumers can then store music files on their computer. Similar compression techniques are now available to create VHS quality digital videos, with CD quality sound, for delivery over the Internet.

226 Decision of the Copyright Board, *Statement of the Royalties to be Collected for the Performance or the Communication by Telecommunication, in Canada, of Music or Dramatico-Musical Works,* October 27, 1999.

This case involved the payment of royalties to the Society of Composers, Authors and Publishers of Music of Canada, (SOCAN)[227] under SOCAN's Tariff 22 (Transmission of Musical Works to Subscribers via a Telecommunications Service) commonly referred to as the "Internet music use tariff" as the primary target of the Tariff was the communication of works over the Internet. Collectives like SOCAN submit draft "tariffs" to the Copyright Board and, if approved, the tariff imposes an obligation to pay, usually in the form of a percentage of revenues. Tariff 22 proposed to impose a tariff on the Internet Service Providers (ISPs) to pay 25 cents per subscriber if that ISP is not earning money from advertising, and from ISPs that were earning advertising revenues, SOCAN wanted that amount or 3.2 percent of gross revenues, whichever is greater.

Most of the music sites like MP3.com are in the U.S. and therefore not subject to the Board's jurisdiction. The only opportunity, then, for SOCAN to collect significant revenues from Internet activity is to collect from Canadian based ISPs in the same manner that it collects from commercial radio stations and television broadcasters.

The issues addressed by the Board included, among others:[228]

1. whether there is a communication by telecommunication to the public when a musical work is electronically transmitted, made available, uploaded, downloaded or browsed;

---

227 The equivalent in the U.S. are Broadcast Music Inc. (BMI) and the American Society of Composers, Authors and Publishers (ASCAP).

228 Decision of the Copyright Board, *Statement of the Royalties to be Collected for the Performance or the Communication by Telecommunication, in Canada, of Music or Dramatico-Musical Works*, October 27, 1999, at 2.

2. if there is a communication, who effects it, who is liable for it and whether anyone can claim the exemption in subsection 2.4(1)(b) of the Copyright Act;[229]

3. the circumstances in which a communication occurs in Canada; and

4. whether the Board may approve a tariff applicable to persons located outside Canada.

The Canadian Motion Distributors Association (CMPDA) and the Canadian Recording Industry Association (CRIA) supported the position taken by SOCAN, arguing that a communication to the public occurs when the end user can access a musical work, thereby imposing liability on the ISPs. They also sought to impose liability on everyone else involved in the Internet chain, including those who provide the transmission services.

The Board described the process for the transmission of music over the Internet:[230]

> When an audio file is sent over the Internet, it is generally converted into digital form, compressed, transmitted, decompressed and reconverted into analog sound signals. ...Generally speaking, information transmitted over the Internet is delivered in a unicast pull mode: pull, because the user requests or "pulls" the information when desired and unicast, because packets go to only one recipient.
>
> ...An audio file may be downloaded onto a storage device from which it may later be played by software that interprets

---

229 *Copyright Act*, S.C. 1985 as am. Subsection 2.4(1)(b) of the *Act* reads as follows: "a person whose only act in respect of the communication of a work or other subject-matter to the public consists of providing the means of telecommunication necessary for another person to so communicate the work or other subject-matter does not communicate that work or other subject-matter to the public".

230 Decision of the Copyright Board, *Statement of the Royalties to be Collected for the Performance or the Communication by Telecommunication, in Canada, of Music or Dramatico-Musical Works*, October 27, 1999, at 16-18.

> the file. However, audio files that are encoded and stored on a server may also be accessed by the use of a streaming program such as Real Audio, to create what appears to be a real-time experience.
>
> ...The Internet may be used for a netcast, in which a feed from a live concert is made available from a server. The server and the bandwidth capacity of the entity hosting it limit the number of users able to view the event. Users have access to the event more or less simultaneously. However, unlike traditional forms of broadcasting, a user may receive a program in any part of the world.

To make content such as music, videos, radio or television available on the Internet requires the person supplying the content to have access to the means of connection (the infrastructure components of the Internet) and to disk space on one or more servers. Depending on the size of the enterprise, the content provider may or may not own or control the server. Smaller businesses usually pay for the right to place information on the server. In these circumstances, the person or business operating the website has a user identification and password provided by the operator of the server and a connection that allows the person operating the website to post content on its website. The server merely operates as a host to the website, and usually takes no control over content, unless in response to a complaint.

From a legal perspective, and for the purpose of imposing tariffs on the "communication" of works, the Board analyzed what occurs on the Internet as follows:[231]

1. A musical work is not 'communicated' (to make known or convey information) when it is made available on a server (whether a host, cache or mirror server), rather it is communicated when the server responds to a

---

231 Decision of the Copyright Board, *Statement of the Royalties to be Collected for the Performance or the Communication by Telecommunication, in Canada, of Music or Dramatico-Musical Works*, October 27, 1999, at 26.

request by a user and packets are transmitted over the Internet for that person to see, hear or copy the work. ISPs are therefore transmitting musical works and potentially liable under the Act.

2. Internet intermediaries, such as the ISP of the person who makes the work available, persons whose servers act as the cache or mirror, the recipient's ISP and those who operate routers used in the transmission can, provided they limit themselves to acting as intermediaries, avail themselves of the 'common carrier' exemption in paragraph 2.4(1)(b) of the *Act* and therefore do not 'communicate' the work.

3. By making a work available, a person 'authorizes' its communication, which is a separate protected use under the Act.

4. The work is 'made available' only when it is communicated, as in number 1 above, however it is 'authorized' when the work is made available or posted on an Internet website. Therefore, the person that posts the material on the Internet is the one authorizing the communication, and consequently liable under the Act.

5. The person that creates an *automatic* or imbedded hyperlink to a work authorizes the communication of the work from the site to which the link leads. The person that merely supplies a link, which must be activated by the user, does not.

This is a positive decision for Internet Service Providers. If liable for music transmission on the Internet, they may also be liable for written works on the Internet,

opening them up to potentially much larger liability for copyright infringement and possibly defamation claims.

In the U.S., ISPs do not pay copyright tariffs to music collectives provided they fulfill certain obligations under the *Digital Millennium Copyright Act of 1998*.[232] Under that Act, ISPs are exempt from paying the tariffs provided they agree to 'unplug' any website that is playing unauthorized music, if requested to do so. In the U.S., and now in Canada as a result of this decision, music collectives must look to the website operators to collect their tariffs.

In analyzing the jurisdictional question, the Board looked at all possible candidates for establishing jurisdiction: the location of the web server hosting the content, the origin of the request, the location of the person posting the content and the location of the original website. The Board rejected all locations except that of the web server as irrelevant for determining jurisdiction. The Board tied its jurisdiction to impose copyright tariffs strictly to the location of the web server hosting the content, on the basis that the communications occur where the transmission originates. Therefore, to be characterized as a "communication in Canada", and thus be subject to the tariff imposed by SOCAN, the server must be located in Canada.

If a Canadian resident posts the work on a server in the U.S., the Board stated that it has no jurisdiction over that individual. Conversely, the Board held that a foreign resident posting a musical work on a Canadian-based server requires a license to communicate the work. Whether the site is where the original material was posted or a mirror

---

232 *Digital Millennium Copyright Act of 1998*, Pub.L. 105-304, Oct.28, 1998, 112 Stat. 2860; 17 USCA sections 1201 - 1332.

site, is irrelevant. If either server (site) is in Canada, the communication occurs in Canada and, according to the Board, a license must be obtained.

It is questionable whether a real and substantial connection exists between Canada and a person who merely operates his website from a server based in Canada, having no other connection with Canada other than to provide access to a piece of music on that site through the Internet. Until this decision, the location of the server was not considered by the courts as a key factor in determining jurisdiction. Is it reasonable for the Board to assume jurisdiction over a U.S. resident in these circumstances and to apply Canada's legislation to foreign businesses? If there are other connecting factors between the operator and the residents of Canada, the result may accord with our sense of 'fair play' but absent such factors, the decision may not be supportable.

Conflict of law questions are also affected by this decision. By stating that the infringing act of communicating to the public occurs when an individual accesses the material from the server, the Board is finding that the laws of Canada will be applied to all communications of music emanating from a server in Canada, and, conversely, that Canada's copyright laws will not be applied to acts of infringement that practically occur in Canada from a server located elsewhere. At present, copyright choice of law rules follow a strictly territorial approach: intellectual property rights are located in the country that granted the rights and can only be infringed by acts occurring there. If a CD containing music subject to copyright interests is distributed in Canada, the rights of the copyright holder are defined by the laws of Canada, where the infringing act of distributing the CD occurred. In the digital environment, however, choosing the correct system of law to be applied is more difficult.

Following the decision of the Copyright Board, the Internet distributor could be liable to pay royalties to SOCAN, on the basis that it is distributing the music in Canada, even if not a single Canadian resident downloads a piece of music. If U.S. residents are accessing the Canadian server to download the music, conflict of law rules would suggest that the copyright laws of the U.S. should also be applied. The choice of which server to engage for carrying the operator's website should be one of the factors, but not the determining factor.

Instant and simultaneous worldwide access to copyrighted works over digital networks fundamentally changes the territoriality notions in copyright and challenges traditional choice of law concepts as determining exactly where the acts of use occur is often difficult. Andreas Reindl, in his article *Choosing Law in Cyberspace: Copyright Conflicts on Global Networks*[233] effectively argues that to promote certainty and predictability in the choosing of the copyright law applicable to acts of exploitation, choice of law rules should use the location of the user as the principal factor to determine the applicable copyright law. Where the exploitation of the work on the Internet has an identifiable and significant effect on the right holder's economic interests in several countries, the right holder should also be entitled to rely on the copyright laws of the countries in which the work was received if the use of the unauthorized work was for commercial purposes or, if non-commercial, had a substantial effect on his economic interests.

---

233 A. Reindl *Choosing Law in Cyberspace: Copyright Conflicts on Global Networks,* 19 Mich.J. Int'l L. 799 at 800.

(iii) Trademarks

Registered trademarks are protected in Canada under the *Trade Marks Act*[234] and in the U.S. under the *Lantham Act*[235] and the *Federal Trademark Dilution Act of 1985*. Unlike rights created under copyright legislation, which are created solely by statute, trademark rights arise both by statute and to a lesser extent under the common law tort of "passing off". The owner of a trademark registered in Canada has, in addition to other rights, the sole right in Canada to use that trademark in association with the products or services for which it was registered.[236] As with copyright, the rights are territorial.

If a Canadian resident uses a domain name or a trademark that, while not infringing any trademark rights in Canada, is actually the same as or confusingly similar to a trademark or trade name used outside of Canada he runs the risk of being sued in, and found liable under the laws of, any jurisdiction where the plaintiff has trademark rights. As discussed earlier, the foreign country's willingness to take jurisdiction would depend on whether that country considered the legislation to be in the public's interest (rather than a private matter between the parties), whether the defendant was a 'cybersquatter' and finally, whether there were sufficient contacts with that country to justify haling the defendant into court in that forum.

4. CONCLUSION

States assert two kinds of jurisdiction The first is the authority of the state to insist that a defendant appear and defend a claim brought against it in the courts of that state,

---

234 *Trade-Marks Act,* R.S.C. 1985, c.T-13, as am.

235 *Lantham Act,* 15 U.S.C.

236 *Trade-Marks Act,* R.S.C. 1985, as am. s. 19.

and second, the authority of the state to regulate conduct by applying its own substantive law to determine the liability of the defendant to the plaintiff. Territoriality used to be a simple, workable principle to define both the adjudicatory and prescriptive jurisdiction of a state. This simple principle has struggled in an era of easy mobility and rapid communication. It is no longer workable in an age where borders are losing relevance.

The volume of trans-global contacts has, as a result of the Internet, increased and will continue to increase exponentially. Inter-jurisdictional conflicts will also rise. The growth of e-commerce will be impeded unless there is clarity, certainty and transparency in the effect of conducting business and other activities on the Internet.

Currently, the trend of the decisions in both the U.S. and Canada is for the courts to assume both adjudicative and prescriptive jurisdiction based on little more than the 'effects test' if the legislation, law or regulation sought to be enforced is one involving a 'protection of the public'. This is becoming readily apparent in the areas of criminal activity, quasi-criminal activity such as gambling, and in highly regulated consumer protection areas such as securities legislation and the provision of healthcare services. In all of these areas, it is unlikely that the courts will require that the defendant have either 'minimum contacts' with the state, or a 'real and substantial connection'. If the defendant's website is accessible to residents of the forum and its out of state activity results in harmful effects in the forum, it is likely that the courts in that forum will assume jurisdiction over the defendant and apply its own laws to the conduct. In the criminal and quasi-criminal areas, this is often referred to as a 'real and substantial link' between the conduct and the forum.

In strictly private disputes, such as a breach of contract action or trademark dispute (other than one involving a cybersquatter), the courts generally look first to ensure that the cause of action arises from the Internet activity and, if that connection is found, they will address whether there are sufficient additional contacts to justify the assumption of jurisdiction over the defendant.

Although a dispute arising from the intentional or negligent act of the defendant would at first appear to be a private action attracting the general principles referred to above, there appears to be an element of 'public interest protection' which enters into the determination of both adjudicatory and prescriptive jurisdiction. For example, if damages are caused to the plaintiff from a tort committed by the defendant, it is probable that the state where the damage is caused (often the plaintiff's residence) will assume jurisdiction and apply its laws. Operating a passive website with content that defames the plaintiff is likely not a sufficient connection for the courts to assume jurisdiction. However, if medical advice is given on a website which is accessed in the forum, the result of which causes the plaintiff harm, it is likely that the ability of the plaintiff to access the advice in the forum would be a sufficient connection for jurisdictional purposes.

When dealing with infringement of a plaintiff's copyright, international treaties state that all rights to copyright in a work are given to the creator by the law of the jurisdiction where the infringement is claimed. When dealing with the Internet, the major problem is to determine where the infringement occurred.

Can these issues be dealt with adequately by the courts without crippling freedom of expression or hampering commerce or the flow of information on the Internet?

Allan Stein suggests that "the new technology of cyberspace does not, in general, confound our basic jurisdictional instincts".[237] In fact, he argues that the courts are developing "a more or less coherent approach to the allocation of judicial authority over cyberspace controversies" and that accordingly, no fundamental paradigm shift is required to deal with this relatively new phenomenon.

Some authors suggest taking Internet disputes away from the regular courts and submitting them to "Internet courts" specifically created to resolve disputes in cyberspace,[238] while others suggest that the best way to move forward is by multilateral agreement leading to an international convention.[239]

While these solutions may be appropriate for regulating illegal conduct over the Internet, or offer the ability to provide a global solution to consumer product type legislation, they do not appear to be required in order for our courts to adequately react to the jurisdictional issues posed by the advent of the Internet. As stated by one commentator:[240]

> ... the challenges, created by the global information revolution are to the conflicts lawyer, matters of degree not substance. The speed, ease and ubiquity of access to protected materials promises an exponential growth in the number of cases in which the conflict of laws is relied upon to mediate between conflicting laws and jurisdictions. But the problems thus

---

237 Allan R. Stein, "The Unexceptional Problem of Jurisdiction in Cyberspace" (Winter, 1998) Vol. 32 No. 4 Int'l. Lawyer 1167 at 1191.

238 Matthew Burnstein, "A Global Network in a Compartmentalised Legal Environment" in K. Boele-Woelki and C. Kessedejian (eds.), *Internet: Which court decides? Which law applies?* (Kluwer Law International, 1997).

239 Lillian Edwards, "Defamation and the Internet" in L. Edwards and C. Waelde (eds.), *Law & the Internet: regulating cyberspace* (Oxford: Hart Publishing, 1997).

240 R. Fentiman, "Conflict of Law in Cyberspace" International Federation of Computer Law Associations, Multimedia and the Internet Global Challenges for Law (Brussells 1996) at 28.

> revealed - of cost, inefficiency, unfairness - are not new, being inherent in a world of legal diversity.

It is expected that the courts will develop appropriate rules relating to the exercise of jurisdiction, which, in most cases, will adequately address the issues raised by commerce conducted on the Internet. It would be helpful, however, if Parliament and the provinces would take the initiative to create certainty where possible, for example in the areas proposed in the draft *Uniform Electronic Commerce Act* and in the proposed *Uniform Court Jurisdiction and Proceedings Transfer Act*. There is also a need for the international community to create certainty in the protection of copyright by creating an internationally accepted basis for determining jurisdiction and choice of law when an act of use or infringement occurs on the Internet. Although these initiatives take time, they are important to our new, Internet based economy, and should be given priority. In any event, it will be extremely interesting to witness how legal systems around the planet will ultimately 'come to grips' with the issues created by the Internet.